The Incredible True Story of the Largest Sting Operation Ever

DARK WIRE

Joseph Cox

The Incredible True Story of the
Largest Sting Operation Ever

DARK WIRE

Joseph Cox

PUBLICAFFAIRS
New York

Copyright © 2024 by Joseph Cox

Cover design by Pete Garceau
Cover images © iStock/Getty Images
Cover copyright © 2024 by Hachette Book Group, Inc.

Hachette Book Group supports the right to free expression and the value of copyright. The purpose of copyright is to encourage writers and artists to produce the creative works that enrich our culture.

The scanning, uploading, and distribution of this book without permission is a theft of the author's intellectual property. If you would like permission to use material from the book (other than for review purposes), please contact permissions@hbgusa.com. Thank you for your support of the author's rights.

PublicAffairs
Hachette Book Group
1290 Avenue of the Americas, New York, NY 10104
www.publicaffairsbooks.com
@Public_Affairs

First Edition: June 2024

Published by PublicAffairs, an imprint of Hachette Book Group, Inc. The PublicAffairs name and logo is a registered trademark of the Hachette Book Group.

The Hachette Speakers Bureau provides a wide range of authors for speaking events. To find out more, go to hachettespeakersbureau.com or email HachetteSpeakers@hbgusa.com.

PublicAffairs books may be purchased in bulk for business, educational, or promotional use. For more information, please contact your local bookseller or the Hachette Book Group Special Markets Department at special.markets@hbgusa.com.

The publisher is not responsible for websites (or their content) that are not owned by the publisher.

Print book interior design by Amy Quinn.

Library of Congress Cataloging-in-Publication Data
Names: Cox, Joseph (Journalist), author.
Title: Dark wire : the incredible true story of the largest sting operation in history / Joseph Cox.
Description: New York : PublicAffairs, 2024. | Includes bibliographical references.
Identifiers: LCCN 2023044541 | ISBN 9781541702691 (hardcover) | ISBN 9781541702714 (ebook)
Subjects: LCSH: Undercover operations—International cooperation. | Electronic surveillance—International cooperation. | Text messaging (Cell phone systems)—Security measures. | Organized crime investigation.
Classification: LCC HV8080.U5 C58 2024 | DDC 363.2/32—dc23/eng/20240130
LC record available at https://lccn.loc.gov/2023044541

ISBNs: 9781541702691 (hardcover), 9781541702714 (ebook)

E3-20240412-JV-NF-ORI

Contents

Cover
Title Page
Copyright

Act I

Chapter 1. ODOG
Chapter 2. The First Window
Chapter 3. Boxes of Phantoms
Chapter 4. The Facebook Gangster
Chapter 5. Ramos
Chapter 6. Operation Safecracking
Chapter 7. Face-to-Face
Chapter 8. The Capturing of Vincent Ramos
Chapter 9. Vacuum

Act II

Chapter 10. Anom
Chapter 11. Roll Out
Chapter 12. Hoops
Chapter 13. Batman
Chapter 14. Kings Cross
Chapter 15. Microsoft

Act III

Chapter 16. Encrochat
Chapter 17. “We Move Anom Like We Move Kilos”
Chapter 18. “Let’s Make Millions”
Chapter 19. Wasta
Chapter 20. The Bridge
Chapter 21. A Cottage Industry
Chapter 22. The Raid
Chapter 23. Metallic Maze
Chapter 24. Hawala
Chapter 25. Black Boxes

Act IV

Chapter 26. Juggernaut
Chapter 27. Squeezed
Chapter 28. Green Light
Chapter 29. Hydra
Chapter 30. Mancuso Luck
Chapter 31. Dominoes
Chapter 32. Reveal
Epilogue

Photos
A Note on Sourcing
Acknowledgments
Discover More
About the Author

Praise for Dark Wire

Notes

Explore book giveaways, sneak peeks, deals, and more.

Tap here to learn more.

PUBLICAFFAIRS

Act I

Chapter 1

ODOG

In the early morning of September 9, 2015, Owen Hanson opened his Louis Vuitton bag and stuffed it with bundles of cash and three cell phones. The money was for gambling during the round of golf he was scheduled to have that day with a business associate. The phones were for orchestrating his dual empires: multimillion-dollar gambling and drug smuggling. He packed his golf clubs into his matte black Porsche, placed the bag on the passenger seat, and started the drive to the golf course.

Hanson didn't look like a typical golf player of the time. Steroid use, intense workouts, and a spot on the University of Southern California football team years earlier gave him a John Cena–like physique more suited to a professional fighter. As he got into performance-enhancing drugs at USC in around 2004, he started to deal them as well, to a list of clients that included professional athletes. Before long, Hanson moved on to selling recreational narcotics, like cocaine and ecstasy. After the 2008 financial crisis he was at the helm of BetODog, his illegal gambling enterprise that took bets on every sport from the NBA to the NFL.

One betting client worked for the Sinaloa drug cartel. That relationship snowballed into Hanson moving cash for the Sinaloa contact across San Diego and Los Angeles. Southern California was a great place to be a drug dealer, given its proximity to the Mexico-US border, and offered plenty of space for promotions. At a blistering speed from 2012 onward, Hanson leapfrogged into wholesale drug trafficking. He shipped cocaine to Australia, where a kilo was worth a massive eight times what it cost in the US. For drug traffickers, Australia was a gold mine. There were hurdles to

getting the drugs in, but if they did get in, smugglers faced a massive payday. Hanson was part of this gold rush himself. His latest deal was to sell five kilograms of methamphetamine to the business associate he was about to play golf with, a man named Al Wilson.

When Hanson was looking for ways to launder the proceeds of his criminal activities from Australia back into the US, he used some unconventional methods, such as smuggling gold coins hidden in UGG boots. He also cashed out drug proceeds through casinos. Wilson, a money launderer, suggested he wanted to work with Hanson.

Hanson first met Wilson at another golf course in early 2015, when one of Hanson's Australian contacts introduced them. After a round of golf, Hanson, Wilson, and two of Wilson's crew hit a bar in a country club. Wilson pulled out his phone, a modified BlackBerry that only sent encrypted text messages. This made it impossible for law enforcement to wiretap the phone in any traditional way. All the cops would have seen was gibberish, a garble of digits, letters, or symbols that masked what the text message actually said. The device went further still and had the camera, microphone, and GPS removed. The phone really wasn't much of a phone at all; it couldn't make voice calls. Hanson recognized the type of phone when Wilson pulled it out because it was the same brand of encrypted phone he used. Hanson's Sinaloa contact had refused to work with him unless he got one. "Anybody who has a phone is obviously in the world of crime," Hanson later said, recalling his reaction to seeing Wilson's device. Al Wilson looked like the real deal. And he was more than just a money launderer. He wanted to traffic drugs with Hanson.

Hanson still needed a bit more convincing before jumping into business with Wilson. The company that made the custom phones was Phantom Secure, with its head in Vancouver, Canada, and with resellers spread around the world. These resellers acted as both vendors and gatekeepers. Phantom Secure's workers sold phones to people if they were referred by an existing customer, which kept the client base mostly isolated to criminals.

Hanson asked Michael Gamboa, also known as Chino, one of Phantom Secure's distributors in Los Angeles, to check how exactly Wilson had managed to get one of the encrypted phones. Chino was Hanson's main contact at Phantom Secure and sold him around three phones a year for many years.

"Chino, I'm not going to do business with these guys unless you can verify that they have been referred by one of you guys, and that they're legitimate," Hanson said. What if Wilson wasn't a criminal at all and was instead a law enforcement agent trying to trap him?

In response, Chino shut down Wilson's Phantom Secure device as a precaution and then set about finding out who these people were. Chino contacted Wilson's crew: Who were you referred by? he asked. The group said they were directed to Phantom Secure by another criminal gang out of San Francisco that was in the marijuana business. Phantom Secure had been working with that group for years.

About two hours after Hanson's request, Chino came back to Hanson: these guys were on the up and up, don't worry.

That was enough for Hanson. He was in.

Hanson told Wilson he felt better after hearing from his Phantom Secure guys that he had been with the company for a year.

"All good, now let's go earn," Hanson wrote to Wilson.

As soon as Hanson got Chino's confirmation, he sent one of his runners to deliver five kilograms of cocaine to Wilson in the pair's first deal in September 2015. The two agreed the deal would take place at a hotel in Del Mar, a town in California, for $90,000. He later followed up with five kilograms of methamphetamine. Hanson and Wilson were in business.

Hanson had anywhere from five to fifteen of his own crew using encrypted phones at any one time. Those members were on a closed network, which meant they could only message one another on their special devices. Almost no outsiders were able to text them, and vice versa, keeping them more secure from investigators. Hanson told Wilson to buy a couple more new phones so he could join Hanson's dedicated network. Hanson didn't want to use whatever network Wilson was already on. He was part of Hanson's inner circle now.

Like Wilson, Hanson flashed his encrypted phone too. This was his contact in Australia, another in Italy, another in Mexico, he showed an

associate. Hanson picked the handle Don Corleone; he was obsessed with classic gangster films and TV. When he partied with a former NFL star, he wore a T-shirt memorializing the crime epic *Goodfellas*. The logo for his gambling organization included a nod to the iconic opening sequence of *The Sopranos*, and *The Godfather*.

Those stories were works of fiction. Through sheer force of will, Hanson turned his fixation with Hollywood's gangsters into a reality. He poured over a million dollars into a restaurant with what he described as a "wise guy room," which had a whiskey bar, poker table, wine collection, and ventilated section for smoking cigars indoors. At one of his homes he kept a silver-plated AK-47, also with a Louis Vuitton logo, that he boasted about to friends. The closest thing to a real criminal mentor in his life was Jan Portocarrero, the head of a gambling organization that Hanson betted with as a customer before creating his own. Portocarrero did resort to violence at times, but he was not a drug trafficker or smuggler. Without anyone to introduce him to those businesses, Hanson used crime movies as his template, and took the violence and intimidation much further. On at least one occasion he hired an enforcer on an hourly wage to beat up a client who failed to pay what they owed. To one person, who he believed owed him $2.5 million, a video was sent of two attackers murdering another two men. One of the killers started to behead the first bound victim with a chainsaw. The second attacker then decapitated the next victim with a knife. A message in the video read, "If you don't pay us money, this will happen to you." After that, the person who'd received the video started to find a way to pay back Hanson in earnest. The message, through the gratuitous violence of a cartel-style video, had gotten through.

Hanson felt something was off even before he got into his Porsche. The night before, his drug boss in Mexico had sent him an ominous message, using their own encrypted phone: "You're about to meet the DEA agents at the golf course," the boss, whom Hanson called El Jefe, wrote. They were suspicious because of Wilson's request for Hanson to specifically provide

methamphetamine a few days earlier. Hanson had never sold meth before, but meth was the drug that Wilson wanted to buy. To El Jefe, that was a red flag. Meth, El Jefe thought, led to harsher prison sentences in the US. One of Hanson's workers was able to secure the meth from the Mexican contacts without much effort at all, but El Jefe was still suspicious.

Hanson arrived at the golf course at around 6:30 a.m. and saw a white F-350 pickup truck in the parking lot. Odd, he thought: when patrons are paying $400 per round of golf, usually they had more expensive cars than that. Except for the pickup, the car park was eerily empty.

Hanson was still forty-five minutes early for his meeting with Wilson so he drove to a nearby McDonald's to get some breakfast. He ordered two Egg McMuffins and an iced coffee, but after the message from El Jefe, he didn't have the stomach for it.

Hanson didn't have to stay in the US. He owned properties in Peru and Costa Rica. One home included a room dedicated only to storing expensive bottles of tequila. Another property had a hidden compartment underneath a bathtub for hiding the spoils of his trafficking. Hanson was building a $2 million house in Cabo San Lucas, a party city in Mexico. He had a fake Mexican ID, and, through his Mexican wife's family, he was getting a fraudulent Mexican passport. Hanson had gotten close to Wilson and told him much of this. El Jefe even suggested Hanson flee to Mexico the night before his planned golf meet. "Just get down to Mexico, it's your best option," they wrote in another encrypted text message.

But here Hanson was, driving back to the golf course despite the warning signs and his own gut telling him something was wrong. In the car park, Hanson brought his Porsche to a standstill.

Elsewhere in the parking lot in a far-off vehicle sat Mick Mullally, an officer from New South Wales (NSW), Australia, organized crime squad. For four years, Mullally had been investigating Hanson and his dealings in Australia. Now that work was finally coming to a head as Mullally waited with the FBI to strike.

As Hanson went to grab his bag from the front seat of his Porsche, he turned around. That's when law enforcement agents swarmed him, guns drawn. Hanson thought he noticed a helicopter whizzing above. Mullally, not able to lay hands on Hanson because this wasn't the Australian's

jurisdiction, stood nearby as the US agents descended. “I was lapping it up,” Mullally later recalled with a laugh.

In the distance, Hanson saw more agents put Wilson in handcuffs. “Don’t say a word to him,” the agents said, as if Wilson were Hanson’s accomplice.

That’s when Hanson realized that Wilson was a setup. “I knew right away it was all an act,” Hanson later recalled. The bonding over drinks and golf. Wilson’s story that he wanted to work with Hanson. The recent handshakes over drug deals. None of it was real. Instead, Wilson’s behavior was a fabrication designed to catch Hanson right in the act of serious drug trafficking. That was why Wilson had asked Hanson to sell him multiple kilograms of cocaine and methamphetamine. As was now clear, El Jefe was right that Hanson was about to meet a bunch of investigators. El Jefe just got the agency wrong: the officials who arrested Hanson weren’t from the DEA. They were from the San Diego FBI.

Most ironically of all, one of the main things that Hanson relied on for his security while trafficking drugs—his encrypted phone—was the detail that convinced him that Wilson was a crime figure and not an FBI agent.

Phantom Secure, the company that designed the custom phones, had a special feature where its staff could remotely wipe a client’s device if it fell into the wrong hands, such as the agents who had just pounced on Hanson. If the agents had any hope of reading the messages stored on Hanson’s phone, they had to copy them before Phantom Secure inevitably issued a wipe command. Because the phone only sent encrypted text messages, the FBI had not been able to get a wiretap and listen in to Hanson’s conversations about the drug smuggling side of his business. There was also the fear that the phone might run out of battery, and no one knew whether the agents could gain access to its contents after that. This was the agents’ one shot at finally being able to read Hanson’s messages on the phone. Without those, the authorities could not understand, or prosecute, the true extent of Hanson’s drug trafficking. In this race, the FBI may have needed to rush the phone to a secure facility through the morning’s traffic. Phantom Secure’s wipe command could travel across the internet nearly instantaneously. The latter had a distinct advantage.

One of Hanson’s crew members told Phantom Secure to wipe the phone after they realized their boss was in trouble. Hanson’s messages may yet fall

through the FBI's fingers. Phantom Secure pushed the button.

But the wipe command never arrived. The messages on the phone remained intact.

FBI protocol said that seized phones should be put into a Faraday bag, a small pocket with metallic lining that blocked any signals getting to, or out from, the device. That included the order to wipe the phone. The FBI successfully relayed the device to its secure location before any command could be received. The agents won the race. Hanson's phone ended up in an evidence room along a white corridor in the San Diego field office.

But there was still a hitch. Hanson's phone was locked by a passcode. Until the FBI could figure out that passcode, the vault of Hanson's messages remained steadfastly locked. Having a safe in front of them is not much use to investigators if they can't unlock it and see the secrets inside.

Through Wilson's interactions with Hanson, the FBI knew Phantom Secure phones shipped to customers with a default passcode. Users were encouraged to change it to something only they knew, so only they could access their phone's contents. Hanson had not followed that advice. He had gotten this Phantom Secure phone to replace another just a short while earlier and had not yet changed the passcode. The authorities entered the default passcode and the device digitally popped open. It was as if Hanson had not bothered to change the combination to his safe from "0000" after buying it.

Meanwhile, after the authorities arrested Hanson in the parking lot, an FBI agent and Mullally immediately escorted their suspect to an interrogation room in Carlsbad, the city near San Diego where he had been playing golf. Mullally sat in the front passenger seat of the Ford sedan while the FBI agent drove. Mullally deliberately kept quiet, knowing his Australian accent would reveal to Hanson there was a bigger picture in play than just the FBI.

Hanson remembered the advice his lawyer had given him: "never to say anything, and ask for my legal counsel." Once inside the interrogation room, Hanson sat in the chair with the table in front of him as the agents brought him water. Then, Mullally spoke. This one, Hanson realized, wasn't American. He explained he was an NSW officer from Australia, where Hanson was part of the drug trafficker gold rush. This wasn't just an FBI operation.

Once Mullally spoke, Hanson had one last thing to say: “This is where I tell you, I want my lawyer and I’m not saying a word.”

Chapter 2

The First Window

It was game night. The Thursday evening after Hanson's arrest, bald and bearded Andrew Young and a handful of other government officials walked into a San Diego sports bar. The multistory hangout called the Tipsy Crow was just a ten-minute walk from the US Attorney's Office for the Southern District of California where Young worked as a prosecutor. Originally from a town of four hundred people in New Hampshire, Young was at the bar to watch his New England Patriots play.

The group of prosecutors and federal agents walked up the steps to the second level of the bar and got their beers. As they stood near a set of couches and a pool table, the football game blared from TVs hanging on the wall. Young got to chatting with Ben Katz, another prosecutor who, by complete happenstance, was also from New Hampshire. California was about as far from home as both could get inside the continental United States.

During the game's huddles and commercial breaks, the pair spoke about work. In a hushed tone, Young revealed he had a gambling case fall into his lap. Young had just moved to San Diego after working as a trial attorney based out of DC. Being the new guy meant being saddled with the work no one else wanted. A superior gave the file to Young on the first day he joined the San Diego office because, frankly, nobody wanted sports racket cases. They were usually crummy gigs. Often the Department of Justice didn't even bother to investigate gambling rings.

But as Young dug into the case, it became clear this one was different: the case revolved around someone called Owen Hanson, a former USC

footballer who had turned to running a betting organization. The FBI first investigated Macho Sports, the gambling ring run by Hanson's mentor Portocarrero. The FBI then got interested in Hanson because his own spin-off organization was particularly violent when it came to collecting betters' debts. Hanson was a colorful character in his own right and was associating with NFL athletes. As a huge NFL fan, that obviously jumped out to Young.

Investigators also suspected Hanson had a side hustle smuggling drugs. But because Hanson used an unusual type of encrypted phone, the FBI's wiretaps hadn't been able to fully penetrate that side of his business. It wasn't clear at what sort of scale Hanson was dealing drugs for the moment.

Young's superiors originally split the case into two parts—the gambling and the drug dealing—and assigned him the former. A drug prosecutor was given the other; however, he had to travel to work on an unrelated trial. The drug prosecutor asked Young, Can you babysit the narcotics side of this Hanson case too, while I'm gone?

Young obliged, but he didn't know anything about running a drugs case. Young was a white-collar prosecutor. After getting into Georgetown University in Washington, DC, Young had joined the Tax Division of the Department of Justice and litigated cases across New York and Philadelphia. He lived for the performance of the courtroom. He compared it to a partly unscripted play, where he was the director, actor, and writer all at once. On the fly, he might have to react to something the other side has done and try to outwit them. In one case he bantered with the judge, who made jokes about Young's bald head. Young found few things more exhilarating than waiting for a jury to read their verdict when nobody knew which way it would go. The courtroom made Young feel alive.

Even if he might later get to run his own stage play in the Hanson case, the world of tax law was a million miles away from the gambling and possible drug trafficking Hanson was suspected of. So Young sat down and learned everything he could about prosecuting a drug case while the colleague was gone.

As Young peeled back the layers of Hanson's organization, he got invested in the case. "I don't want to babysit this. I want the whole thing," Young later recalled. By the time the prosecutor returned, Young asked if he could take the entire case. Run with it, the prosecutor said.

With Hanson under arrest, Young now had more work to do on both the gambling and the drugs cases. He had to dig through the messages on Hanson's encrypted phone to determine the true scale of his crimes. And Young needed to identify the other members of Hanson's criminal enterprise so they could be arrested too.

In the sports bar as the New England Patriots game continued, Katz talked about the likely odds of the match. Katz loved to gamble on sports—$50 a game, those sorts of low-stakes, fun bets. He wasn't gambling that night because he only bet when legally able to, like in Vegas. But as Katz reeled off points and odds, Young saw that he clearly knew his way around the gambling world. That knowledge could certainly come in useful in the Hanson investigation. Young asked Katz if he wanted to help out on it.

At that point, Young could have offered Katz a boring tax avoidance case and he probably still would have said yes. At work, Katz was stuck in the department that only handled border cases. A never-ending treadmill of low-level drug smuggling and immigration offenses. A depressing churn where prosecutors most often doled out prewritten plea deals to underprivileged and overlooked parts of society. Those prosecutions didn't make any real impact beyond raking up stats for border enforcement. That was how some from other districts saw San Diego: the little brother of Los Angeles that policed the border so the LA prosecutors didn't have to. An underdog mentality permeated some of the staff in San Diego.

Katz wanted to do more stuff that mattered. He hoped to get onto fraud cases, like the ones Young's department worked on. This pitch was even better: a chance to work on something fresh with a fellow New Hampshire boy, and the Hanson case was obviously not your everyday investigation. It might even be fun.

Katz had his answer. He told Young, "I'm in."

Young and Katz sat in their respective offices in the US Attorney's Office, and each looked at two computer monitors side by side. On one, both investigators rummaged through JPEGs of Hanson's Phantom Secure

device, a new treasure trove of data showing exactly what Hanson had been up to shortly before his arrest in the golf course car park. After the FBI secured the phone, its agents had painstakingly copied every message stored on it. The archiving solution was distinctly low tech: message by message, the FBI scrolled through the device, took a photo of the phone displaying the text, and then scrolled on to the next one. Hanson had only gotten that particular Phantom Secure phone a short period before his arrest, but it contained thousands of messages.

On his second monitor, Katz had the fruits of the wiretap against Hanson's ordinary phone, information that the authorities had already collected before his arrest. Young's second screen, meanwhile, was nearly always open on Google, ready to dig up other information on the members of Hanson's crew. It was now Katz and Young's job to make sense of Hanson's encrypted messages. Hanson would soon face charges of methamphetamine trafficking because of the undercover operation involving Wilson. But this phone was where the prosecutors' work really started.

The US Attorney's Office for the Southern District of California where the pair did this work was a depressing sight. The squat, multistory building's exterior was, by Katz's description, a crash course in brutalist architecture. The building inelegantly straddled a road. It could easily pass for the DMV. The building was attached to the San Diego district courthouse, meaning that whenever the attorneys needed to have a document signed, they could dash over and get a judge's signature quickly.

Inside, the carpets were dingy. Documents in beige folders sometimes piled up on bookshelves, tables, and in boxes on the floor. In Katz's office, beyond the desk and two computer monitors were a couple of uncomfortable guest chairs and some beat-up metal filing cabinets that contained his physical case files. Some prosecutors decorated the sparse walls with legal diplomas.

For months, much of Young and Katz's days and nights consisted of reading through Hanson's Phantom Secure messages and mapping the spiderweb of Hanson's criminal network. Like the FBI before them, they scrolled through Hanson's now archived messages one by one. Every night, Young went through a couple of hundred and looked for clues. In one example, he found a person who was referred to as "Candy Store." A few

thousand photos later, and there was Hanson's list of contacts. "Candy Store" had an address listed next to it. Young looked up the address and found a warehouse that belonged to a chocolate import company.

On his Google monitor, Young then dug into the owners, two brothers called Nathan and Andrew—coincidentally the same names as Young and his own sibling. As Young Googled around, he found one of these brothers went to USC at the same time Hanson was there, and that he was a volleyball player, just like Hanson was at one point too.

"Boom," Young thought. "This is the guy."

Hanson used the chocolate import company as an effective cover for his drug smuggling. His crew hid narcotics inside shipments of ordinary items. At one point the packaging was so effective that Hanson's underlings tasked with unloading the drugs couldn't find them. In Phantom Secure messages, the crew told Hanson the drugs weren't there. (They were, only they were deeply nestled between the company's legitimate products.) One of Hanson's preferred methods for smuggling cocaine had been by putting the drugs inside wine bottles. His workers then nestled these bottles inside gift baskets. The gift baskets didn't look suspicious, and the bottles themselves had room for nearly exactly a kilogram of cocaine each.

Young repeated that process of uncovering Hanson's contacts over and over. The group appeared to consist of around fifteen to twenty people in total. Young ultimately unmasked at least half of them just based on the contents of the messages. It was the somewhat more modern equivalent of the investigator's blackboard with mug shots and red string. Not that much more modern, though.

Katz, meanwhile, focused on making a timeline. He cross-referenced the Phantom Secure texts with the contents of the earlier wiretap and noted down any significant messages in an ever growing Excel spreadsheet. He could then sort and tweak things into a chronological series of events. Sometimes when he found something interesting, Katz shouted down the hallway for Young to come look. He then walked Young through what he'd discovered.

Katz saw that Hanson would hold one conversation on his normal phone, indicate to an accomplice to move to some other device, and then continue the conversation on the Phantom Secure phone. Those conversations, primarily, were about the drugs side of Hanson's operation.

Through the messages, the true, colossal scope of Hanson's trafficking came into view. Hanson wasn't selling some drugs on the side of his gambling business. Drug trafficking was his business. Thousands of kilos of cocaine from California into Chicago. Hundreds of kilos to Australia. He trafficked heroin too. The Phantom Secure phone made the gambling side of the investigation look quaint. This was no longer all about Hanson's bookkeeping. The investigation was into a prolific international drug trafficker.

In the messages, Hanson's gang talked explicitly about quantities of drugs. Whereas on a normal phone, a criminal might say they planned to ship fifty "tires" or some other innocuous item, on Phantom Secure, they simply said fifty kilos. The messages contained physical addresses of drug drops. Bank account numbers. And identifying details like those Young found for the candy store. The criminals didn't think they needed to bother with many code words; Phantom Secure was protecting them already.

It may have appeared that Hanson was the top of the chain, running his minions through his encrypted phone as they shipped massive quantities of drugs across the world. But the chats showed he was actually the number two. Someone else was above him—the supplier of the drugs. Their identity was unknown. El Jefe remained a ghost.

In the chats, this supplier was smarter and more careful than Hanson. They didn't show off their criminal lifestyle. Instead, the conversations were limited to information about shipments. This was how the pros conducted their business, not like the guys Hanson idolized on TV.

Even if El Jefe got away, the prosecutors had uncovered a mountain of evidence for the next phase of the Hanson case. The FBI was ready to bring in those that the team identified.

At five a.m. on January 27, 2016, the family dog started barking at the country home of Zack.[1] Soon after, Zack heard what he thought were shotgun blasts. He grabbed his own gun and screamed to his intruders through the bedroom door. "I've got a gun. Who is it?" he yelled.

"FBI! Put your guns down!" came the response.

Zack couldn't get rid of his weapon fast enough. He says he threw it in the closet, got down on the floor, and put his hands behind his head. The FBI had turned up to his house with an assault vehicle and what he

estimated to be over two dozen agents. He was one of Hanson's crew members included in the new round of charges, which targeted Hanson's wider gambling and drug trafficking organization.

The initial indictment against Hanson in September was sparse; it alleged that Hanson had conspired to distribute cocaine. The indictment also charged one of Hanson's drug runners. Based on the prosecutor's digging through the Phantom Secure phone and other work, in January 2016 the court unsealed a new indictment against Hanson and nearly two dozen members of his criminal enterprise. Among other things it alleged Hanson distributed hundreds of kilograms of drugs through the US, Australia, and elsewhere. Two years later, the prosecutors indicted the two brothers who owned the chocolate company that helped smuggle some of Hanson's drugs.

Zack, the Hanson crew member raided by the more than two dozen agents, later said, "A phone call would have been fine. I would've gone in."

Hanson's Phantom Secure phone gave up his secrets to the authorities. When they reviewed the communications, the prosecutors determined Hanson had moved over a hundred kilograms of cocaine during and after Labor Day weekend from Los Angeles to Canada. As it turned out, that was not an isolated incident. Hanson said he moved hundreds of kilograms of cocaine per month over the course of several years, from Mexico, to the US, and then to Canada and Australia. The tech that powered every one of those shipments was Phantom Secure phones.

The FBI was already a little familiar with Phantom Secure phones because Wilson, the undercover agent, had used them to trick Hanson in the first place. The FBI, though, were still novices with fully understanding how Phantom Secure and its phones worked. Their agents and technical staff continued to poke around the phone and figure out what they were dealing with.

More than anything, gaining access to Hanson's phone opened the prosecutors' and the FBI's eyes to something beyond this single gang. What

about the potentially thousands upon thousands of other people, also likely criminals, who were using Phantom Secure too? This was bigger than just one drug case, one crew, or one cartel, even one that operated at the massive size Hanson did. The phones were a window to a whole new world of crime, one that the FBI and prosecutors were only just starting to glimpse. Mark Pletcher, one of the other prosecutors inside the US Attorney's Office, said the team should focus on Phantom Secure. In April 2016 police in the Netherlands announced they had targeted an encrypted phone company called Ennetcom and obtained users' messages. That showed the San Diego team maybe a similar motherlode of intelligence existed inside Phantom Secure.

For years, decades, traffickers like Hanson got away with their crimes because of companies like Phantom Secure. It was only Hanson's brazenness, his need to be known and seen as a gangster, that let Young and the FBI catch up with him.

"If Owen hadn't made mistakes, and hadn't been stupid, he never would have gotten caught," Young said.

Not everyone would be as reckless. Other criminals who used encrypted phones and were smarter, like Hanson's supplier across the Mexican border, were never arrested.

The FBI realized that investigating Phantom Secure could be a chance to get those sorts of people. The ones who aren't on the radar. The cunning ones. The people who don't get got.

Rummaging through Hanson's phone planted the seed of an idea: What would it be like to see the messages of all of the users of one of these phone companies? The investigators decided to branch out; they needed to look into Phantom Secure itself.

Footnote

1 Author has changed this person's name.

Chapter 3

Boxes of Phantoms

Around seven years earlier, in 2009, Shafik Punja was at work in his role as an examiner for the Calgary Police Service in Canada when a colleague brought him a sturdy cardboard box. By his own admission, Punja's digital forensics lab looked more like a Best Buy Geek Squad than a stereotypical law enforcement facility. The room had monitors and computers everywhere. Those computers were in various states of disrepair, as he or colleagues pulled hard drives out of them to then mine for useful evidence.

Inside the cardboard box, among a new set of electronic devices for Punja to sift through, were dozens of encrypted BlackBerry devices. Punja had seen enough of these customized phones in his time to immediately know he would have his work cut out for him. By now, he was accustomed to being locked out of their contents. "You have a gut feeling that you're not going to be easily accessing any of the devices that you're going to be examining, specifically, the BlackBerries," Punja said.

Despite the low chance of accessing the dozens of encrypted BlackBerries from the cardboard box, he still diligently got to the task at hand. First he cataloged them into his lab's database, which tracked what devices were in its possession. He laid out each phone one by one on a desk and scanned a related bar code to input them into the system.

Once the phones made their way through the long queue of other devices that had to be analyzed first, Punja looked again at each BlackBerry, this time more closely. He was searching for things that indicated what state the phone was in, because that dictated what forensic

tools he might then use to try to extract data. Was the phone on or off? Did the battery need replacing? Most importantly, hidden inside the phone underneath the battery was sometimes a sticker that showed a company had modified the device. If the phone had one of those stickers, it was often game over for investigators.

Encrypted BlackBerries linked to drug trafficking, weapons smuggling, and the production of counterfeit currency often rolled through Punja's lab. This was the everyday reality for local cops like him, and even for Canadian federal government agencies, which sometimes sent devices to Punja for help. US authorities encountered the phones too.

Organized criminals broadly were evolving and moving onto platforms the police could not access with traditional investigative or forensic techniques. That didn't mean all the crimes were unsolvable—informants and gumshoe detective work still had their place, maybe even more so. But the criminals could talk without fear, and the modified BlackBerries kept their secrets safely locked away even when the cops managed to grab the phones too.

The issue was twofold: The encryption on the messages meant that police couldn't wiretap the phones as they had for over a century. And then another sort of encryption that protected data on the phone itself meant police couldn't access any messages stored on the phone even after seizing it in a raid. Punja's job was to do what he could about the latter.

Around the world, from America to Australia, Mexico to Morocco, more and more criminals turned to these sorts of encrypted phones. And forensics experts, like Punja or his equivalents in other law enforcement agencies, were locked out.

Criminals' obsession with BlackBerries started years before Phantom Secure even existed. BlackBerry Messenger (BBM), the company's own proprietary text messaging platform, was the chat app of choice for gangsters. Crooks knew that ordinary phones were a bad idea. They shouldn't talk about business on an open wire, be that drug trafficking, hits,

or anything else. BlackBerries offered something else: a scrambled text messaging service. To many, BBM was viewed as so secure that the biggest bank in Canada banned many of its staff from sending such messages because it locked bosses out of their workers' communications and caused regulatory issues. Where corporations saw an issue, criminals sensed an opportunity. BlackBerries became the gadget of choice for organized crime, especially in Canada.

Gangsters' constant dodging from their law enforcement pursuers was by its nature a cat-and-mouse game. Often the crooks found a new piece of technology to exploit before the cops caught up. Sometimes the police overstepped and responded with surveillance techniques that laws were not designed for, or that carried their own legal and privacy implications. With cell phones, police turned to so-called Stingrays, suitcase-sized devices that had a habit of interfering with innocent bystanders' phones as well as criminals'.

That dynamic continued with BBM. Behind the veil of BlackBerry's privacy-focused marketing, cops suddenly started to access criminals' communications. Sometimes police obtained these messages on a truly massive scale. Starting in 2010, the Royal Canadian Mounted Police (RCMP) rummaged through over one million BlackBerry messages and used them to investigate, and dismantle, two Italian organized crime groups that operated in Canada (prosecutors eventually dropped charges). The messages detailed every sort of activity a crime ring might get up to, including narcotics smuggling, kidnapping, and stockpiling weapons, and identified gangsters suspected of a series of violent crimes from 2010 to 2012.

This mass interception was possible because BBM had an Achilles' heel. The version of BBM that most BlackBerry users typed away on was protected by a single, global key that handled the encryption of every message. The digital equivalent of a skeleton key, this small piece of code was what BlackBerry used to encrypt every message, and in turn, decrypt them if it chose to. The RCMP obtained this key—never revealing the key's source—and was able to strip the protections of any message sent on the consumer version of BBM that the agency managed to intercept. When the RCMP operation started, BlackBerry had over eighteen million users in the

United States. The key could unlock millions upon millions of safes, only a sliver of them belonging to criminals, if the police so wished.

Smarter gangsters balked at the idea of putting their security in the hands of a mainstream company like BlackBerry. To them, the tech giants were always going to work with the authorities. The better option was to seek out lesser known firms whose operators may cater specifically to their criminal needs.

In 2006 Nathanael "Nat" Lineham ran a company called beStealth, which sold BlackBerry phones and had offices in Orange County, Guadalajara, and Vancouver. Nat marketed beStealth's phones to drug traffickers and distributed them to members of a particular gang. That crew smuggled ecstasy down from Canada into the United States, and then cocaine back the other way. Nat was essentially the tech guy for the crew, who provided the BlackBerries so police couldn't listen in.

Rather than using the consumer version of BlackBerry that the RCMP obtained the global encryption key for, Nat's BlackBerries had their own BlackBerry Enterprise Server (BES). This meant that beStealth used a different key to decrypt and read the messages, and beStealth held the key, not BlackBerry corporate. Having the key put Nat in control; even if BlackBerry wanted to decrypt the messages of Nat's crew for the benefit of law enforcement, it was unable to do so. Only Nat could do that.

BlackBerry intended BES installations to be used by its government and corporate clients. Agencies used them to make it harder for foreign adversaries to snoop on their messages. Businesses set up their own BES because it meant they could, if needed, monitor or review their employees' communications. Nat flipped the script and sold this more robust capability to his drug trafficking contacts.

BeStealth was different from BlackBerry not so much in a technological sense but in a policy one. BlackBerry headquarters was a friendly face to law enforcement. The company was often happy to help, and like many tech firms it had a dedicated support line for law enforcement to submit data requests. BeStealth was the opposite: it was an adversary that appeared to have no interest in providing data about its users. While Punja worked in the Calgary Police Service lab, colleagues brought him more cardboard boxes that this time contained beStealth devices. Based on his and others' direct experience with the phones, in 2009 Punja warned his fellow forensic

experts in a lecture he participated in at a conference in Chicago. “Don’t expect them to help,” he said of beStealth.

US authorities ultimately charged Nat in September 2008 with conspiracy to distribute MDMA, along with profiting by providing BlackBerries to traffickers so they could avoid law enforcement. Nat pleaded guilty, and beStealth was no more.

Around that same year Phantom Secure innovated on top of beStealth by combining the BlackBerry handset with other security tweaks. That included a more robust implementation of encryption that stored keys on users’ own devices. This meant that even if police seized Phantom Secure’s servers, it may not be able to decrypt or read its customers’ messages to one another, at least not without significant cooperation from the company’s owner. Law enforcement had to gain access to an individual device, like the FBI did with Hanson’s Phantom Secure phone.

The progression from BBM to beStealth and then Phantom Secure was not strictly linear. Some criminals still used BBM while others spread out to new options on the market. But what sprang from that lineage was a hypercompetitive industry in its own right—a battle among dozens of firms to be crowned the king of secure comms for organized crime.

This was the criminal underworld’s tech explosion, and it marked the most important technological leap for organized crime since the dawn of the mobile phone. One encrypted phone seller later told an associate to force his customers to use secure devices. He wrote from his own encrypted phone that “it’s not the ’80s anymore and we have to evolve to keep up.” Companies like Phantom Secure did just that. Beyond a handful of investigations, they provided a safe haven from the police. These encrypted phone companies gave organized crime the upper hand. Whereas criminals previously used phones or pagers made by the same companies as everyone else, soon they had their own dedicated tech sector that was happy to release a new phone or feature, not unlike the annual releases of the Apple iPhone. Customers were loyal to their preferred brand and loved innovative new products.

These companies were just as valuable as some of the funding rounds that Silicon Valley startups received. They pulled in tens of millions of dollars of revenue and took buyouts from investors. The industry had its own high rollers, disruptors, up-and-comers, and rock-bottom failures.

Some made enough money to get by, while others skyrocketed to global popularity.

Tech nerds ran some of the companies. Naive businessmen created others. Some international drug traffickers created their own companies, at first to secure their own messages and then later to diversify their revenue streams by selling phones to other criminal syndicates.

Competitors in the phone business hacked one another, stealing their rivals' customer data and dumping it online. Sellers engaged in disinformation campaigns against one another in an attempt to confuse clients and have them switch to another phone provider. The companies charged thousands of dollars for short six-month subscriptions to the phones. From that easy money, the companies' predominantly male distributors partied at private hotel pools surrounded by escorts. Their safe deposit boxes held solid gold bars and other riches. They bought Lamborghinis, Ferraris, and penthouse apartments.

These businessmen pulled in immense wealth while essentially nobody outside of their customer base or law enforcement had ever heard of them. The companies simultaneously lived in obscurity while they became a bedrock to organized crime in nearly every country in the world.

The phones landed everywhere crime syndicates could be found, from cocaine production labs to drug safe houses. The users were corrupt police and government officials, hitmen for hire, and artisanal drug smugglers. Money launderers who cleaned cash across continents. Weapons dealers who handled AK-47s, pistols, and grenades. The Italian Mafia. Asian triads. Outlaw motorcycle gangs. You weren't a serious criminal unless you had an encrypted phone.

Criminals had finally taken a sizable lead in the surveillance arms race.

Phantom Secure was an innovator in this space, but the underground tech industry was still changing, and fast. After the fall of beStealth, Phantom Secure emerged as its accidental successor. At first, its phones were cool-to-have gadgets. Soon, it catapulted to popularity in the criminal world, largely thanks to one man: Hakan Ayik.

Chapter 4

The Facebook Gangster

Hakan Ayik was on the run and needed to slip across the border as smoothly as possible. The car he was in with an associate pulled up to a checkpoint on the Mediterranean island of Cyprus in October 2010. Ayik was coming from the Turkish-occupied north half of the island and trying to cross to the south, into the Republic of Cyprus. The United Nations–patrolled checkpoint saw thousands of people cross legally every day. That wouldn't work for Ayik. He was one of Australia's most wanted criminals.

Australian authorities had cracked down on Ayik's drug trafficking organization and had orchestrated the arrest of one of his business partners in Hong Kong. They had concrete evidence linking Ayik to a shipment of 175 kilograms of heroin, worth more than $50 million, which had arrived in Sydney's Port Botany from Bangkok, Thailand, in July. A warrant was out for Ayik's arrest, and the drug lord decided to flee while on an international trip instead of returning home to Australia. Soon after the operation wrapped, Ayik mocked his pursuers in a Facebook post in Turkish: "Catch me if you can."

Unfortunately for Ayik, he stood out from a crowd. He looked like a bodybuilder, with gargantuan chest, arm, and leg muscles built with years of steroid use. Black tattoos covered his right arm and chest. His shaved head encased two beady brown eyes that in some photos seemed more welcoming than threatening.

When Ayik inched closer to the crossing along the single-file road and handed his passport to border officials, they studied his documents closely. Ayik, nervous, darted back toward the Turkish side. The officials purportedly fired their weapons, and Ayik's vehicle kept going as the bullets missed it.

On December 20, more than a month after his failed border crossing, authorities traced Ayik to a hotel in Kyrenia, a historic port town on the northern coast. When the local police searched Ayik's hotel room, they found drug paraphernalia, including equipment to make steroids, and seized

a laptop and eight mobile phones. A court in the Turkish Republic of Northern Cyprus granted Ayik bail but confiscated his passport and ordered him not to leave the island. There were some potential stumbling blocks—there was no extradition treaty between the de facto state and Australia—but authorities believed this could be their chance to finally get their man.

Dressed in a gray sweater, wide-collared shirt, and a thick coat of five o'clock shadow, Ayik left the courtroom. He then vanished. Ayik went on the run, again. He likely bribed his way out of the country, fled on a ship, and reportedly got to the criminal safe haven of Dubai. As quickly as Ayik had come into Australia's grasp, he slipped through their fingers.

Ayik grew up far from the opulence that would later become one of his trademarks. He was born in Australia to Turkish immigrant parents, and his father died when Ayik was young. Drugs were a part of his life, with several family members suffering with addiction. He got through early education at an all-boys high school near Sydney. During those high school years, Ayik started a friendship with someone who would come to define much of his own life but also that of crime in Australia overall: Duax Hohepa "Dax" Ngakuru, who later became the national president of the outlaw motorcycle gang the Comancheros.

The Comancheros wore black leather vests emblazoned with the gang's logo of a condor on a red, gold, and black background. Jock Ross founded the group in the late 1960s and modeled the organization after paramilitary groups.

The Comancheros had a long history of violence. One particularly bad incident happened in 1984, when their rivalry with the Bandidos motorcycle gang reached fever pitch in the parking lot of a tavern, during a biker and motorcycle swap meet. Police arrested more than thirty people after a massive shootout left seven people dead. One person's arm was chopped off with a machete. Six of those killed were bikers. One victim was a fourteen-year-old girl, an innocent bystander blasted with a .357 rifle.

In 1998, an eighteen-year-old upstart called Mahmoud "Mick" Hawi joined the Comancheros. A few years later, it's been said that he and a handful of other members forcibly retired the group's boss: step aside as leader, or face the consequences. Ross did the former.

Hawi, with his muscles, gold chains, and tattoos, became the new face of the Comancheros. He ramped up the violence further. In 2009 Hawi happened to be on the same flight as Derek Wainohu, the boss of the Hells Angels. After they each got off the plane and rallied their troops, all hell broke loose inside one of the domestic terminals of Sydney Airport. Bystanders were terrified. One Hells Angels biker died after being stabbed and bashed with a metal bollard during the fight.

Hawi had much more ambition for the Comancheros. He brought in other contacts to replace its members, transforming the bikers from a group of haphazard outlaws into a professional drug trafficking organization.

That was where Ayik came in.

There have been reports that Ayik and Hawi both went to the same high school. Eventually Ayik straddled the worlds both in and out of the Comancheros and remained close enough to the organization to influence it. He was able to push the Comancheros in certain directions, especially when it came to distributing drugs.

Professionally, Ayik was a smart businessman, according to one person who worked directly with him. In one case, Ayik planned to make methamphetamine in Asia, where precursor chemicals to manufacture the drug were legal and available in bulk. He would handle the smuggling into Australia. Then Ayik would have the Comancheros and other biker gangs distribute the drugs throughout the country. Ayik essentially outsourced a part of the drug trafficking supply chain to a willing team of contract workers, not entirely unlike Uber hiring independent drivers to ferry passengers in vehicles the company doesn't actually own. Amazon hires third-party businesses and delivery people to ferry customer orders from the tech giant's warehouses to customers' front doors, in what Amazon calls the "Last Mile" program. Ayik's biker connections fulfilled this role too.

As Ayik flooded Australia with drugs, he flaunted his wealth on social media and elsewhere. On Facebook especially he shared clips of his luxury watches; a photo showed him perched on the bonnet of a bright white Audi R8 Spyder, a sportscar worth hundreds of thousands of dollars. His

LinkedIn profile euphemistically said he worked in the “import and export” industry, and that he was interested in “career opportunities, consulting offers, new ventures, job inquiries, expertise requests, business deals, reference requests, getting back in touch.” He got his hands dirty: in one photo posted to social media, Ayik was seen in what was alleged to have been a drug lab, spooning white powder out of a bag and smiling to the camera. Seeing his audacious social media presence, the Australian media dubbed Ayik the Facebook Gangster.

Then police had evidence linking Ayik to the massive heroin shipment. That was when Ayik first went on the run. This was too much heat, even for the man who constantly laughed in the face of it.

As he fled from Australian police, Ayik had a problem. Criminals had a code of not trusting phones, but with Ayik skipping the country, he wouldn’t always be able to meet his business partners in person. He needed a solution to securely communicate with his associates quickly as he bobbed and weaved with law enforcement agencies.

Some people in Australia used a tool called SMS007 made by a Czech company. SMS007 was a Java-based app installed on clunky Nokia, Sony Ericsson, and Siemens handsets, before the advent of true smartphones. The app took ordinary text messages and coated them in a layer of AES encryption. SMS007 was a novel idea when it launched in the Czech Republic in 2005, but it came with a very cumbersome roadblock. Users had to agree on a password beforehand with one another, and only that password could unlock the messages they sent to each other later. It made communication safer but much more difficult.

Ayik found something much better. He came across a company called Phantom Secure. Its phones promised to encrypt its users’ messages and had needless features stripped out. No one had really heard of this device before, but Ayik had a genuine use for such a highly customized device due to his hostile work environment. He ran the device past a tech expert who

went by the nickname Afgoo. Afgoo later became a seller for Phantom Secure himself.

Ayik rolled the dice and put his trust, and ultimately his freedom, into the hands of this unknown device. He "took the leap of faith because he had to. He was on the run and needed a way to manage his people back home," a person who worked directly with Ayik said. For Ayik to speak to his crew securely, they needed the phones too. Ayik distributed Phantom Secure devices to his contacts back in Australia. He conscripted people to set up the phones on his behalf, and then started selling them to more criminals.

Ayik's decision didn't just modernize his own operations. It would forever and radically change organized crime in Australia, and later the world.

After escaping from the Cyprus border in 2010, Ayik dodged law enforcement once again. He spent some time in Barcelona. In 2012, Spanish police monitored a meeting at which they believed Ayik was with Dax, his childhood friend and now former national president of the Comancheros. Spanish police sprang into action but arrested the wrong man. They nabbed Dax instead of Ayik, and Ayik fled once again.

Some fugitives ended up in Thailand or Marbella. Many gangsters preferred the safe haven of Dubai, which had a long history of not extraditing wanted criminals. Eventually, Ayik settled into a new base of operations: Istanbul, Turkey. He harbored connections to corrupt officials there, and its location was a perfect spot for a drug kingpin. To the east, Ayik had countries like India for sourcing precursor chemicals and triad methamphetamine cooks in Asia, whom he traveled to see on a fake passport. Then he had drug trafficking contacts to the west in Europe.

In Turkey he owned multiple properties including one in Kemer Country, a highly exclusive walled-off suburb to the north of Istanbul that offered various communities of apartments and houses in different styles with an adjoined country club and restaurants. He bought and managed a boutique hotel, a legitimate business with rave reviews.

For someone at the helm of a drug trafficking empire, Ayik wasn't above doing some of the more mundane tasks in his hotel. He responded to one review of his hotel that suggested it should switch to a different brand for the shampoo in the rooms. Ayik assured the customer the hotel would look into it. The boss was often helping out the front desk, the workers in the

cafe, and the cleaners and housekeeping staff. He took the workers out for pizza in one of the restaurants in the large shopping mall across the road from the hotel. Ayik seemed to respect them.

Once he fled to Turkey Ayik changed his surname to Reis, Turkish for "chief." It was hardly the best of covers; a group of Australian journalists later found his name change when they searched through Turkish identity and birth records. Most notably, Ayik renounced his Australian citizenship, an extreme step and a clear signal that he was severing his ties with the country, at least officially.

NSW authorities were so desperate to catch up with Ayik that they took out advertisements in at least one Turkish newspaper as part of their hunt. It did not work. Ayik had been on the run for about a decade by now, with only a few speed bumps along the way.

Beyond Australia's borders and out of reach of the police, Ayik conducted his business through the click-clack of a Phantom Secure BlackBerry keyboard. He demonstrated something that encrypted phones like Phantom Secure were uniquely positioned to offer: a modern drug trafficker didn't need to be in the country they were smuggling drugs out of or into. These phones enabled smugglers to control their operations remotely. Drug trafficking was more globalized than ever. He exemplified a new type of criminal who moved effortlessly across borders and enjoyed whatever pleasures and business opportunities a particular country offered.

Ayik continued to smuggle cocaine and methamphetamine into Australia and work with bikers in the country. Giving an indication of the brazen scale at which Ayik continued to operate, in 2014 Australian police seized nearly two tons of MDMA and about one ton of methamphetamine, one of the country's largest ever drug busts. The narcotics were found in a shipping container from Hamburg, hidden among furniture. Those were Ayik's drugs, according to the *Sydney Morning Herald*.

Ayik's introduction of Phantom Secure to Australia happened in the shadows. Phantom Secure's sales in the country were still relatively slow. A

$2,000 phone that could only text wasn't the most attractive sell, and everyone considered phones as inherently insecure, one Phantom Secure distributor said. The seller often gave out free demo phones for potential clients to try, and then found them in the trash bin on the way out.

Then Australia's law enforcement bodies decided to shine a blinding spotlight on the company.

"Uncrackable Phones Provided by Phantom Secure Linked to Murder of Hells Angels Bikies," a March 2014 headline read. Senior law enforcement officials who spoke to Australia's ABC News at the time said encrypted phones were linked to a series of underworld killings in Sydney, including when a member of the Comancheros ordered the hits of a Hells Angels member and an associate using what the feds believed was a Phantom Secure phone, ABC News wrote. In one of those murders a gunman fired a hail of bullets into a car as the victim sat in the driver's seat. ABC News also produced a flashy TV spot, in which Australian cops said, face to camera, that they couldn't get into Phantom Secure's messages. ABC News said it did not suggest that Phantom Secure "is aware its products are being used by criminals, only that criminals have become aware of the phone's utility and have taken advantage."

The ABC News coverage, and Australian law enforcement's deliberate choice to talk about the issue, had an inadvertent effect: Phantom Secure became more popular. The media spotlight "put Phantom on the map," a Phantom Secure distributor recalled.

One Phantom Secure seller took the ABC News TV spot and uploaded it to their own YouTube channel. What was supposed to be a piece of journalism and a cry for help from law enforcement was now an advertisement. Phantom Secure co-opted "uncrackable," the term used in the headline, and used it as the company's own catchphrase. Before long, one seller with a yellow Lamborghini advertised delivery of Phantom Secure phones within thirty minutes anywhere in Sydney's central business district.

In its 2014–2015 annual report, the New South Wales Crime Commission, a part of the government tasked with reducing organized crime in that region of Australia, wrote that "the prolific use of encrypted Blackberry devices continued unabated and, as in previous years, these devices were used to facilitate drug trafficking." The Australian Criminal

Intelligence Commission, a body that operated at the federal level, later pointed specifically to Phantom Secure in one of its own reports as providing phones for outlaw biker gangs and other organized crime groups.

Ayik successfully seeded Phantom Secure in Australia. But only after Australian law enforcement's decision to go loud did every criminal in Australia want one, a Phantom Secure distributor said. Crooks wanted to be like Ayik, and Phantom Secure let them do that. The truthful claim from the Australian authorities that organized criminals were using encrypted phones became a self-fulfilling prophecy.

"The cops made Phantom," one of the company's distributors said. Some customers got tattoos of Phantom Secure on their bodies. Brand recognition soared, and the company's clients in Australia were loyal. In Australia at least, some employees of Phantom Secure didn't do any vetting; the company sold its phones to anyone. In all, the FBI says that Phantom Secure sold many thousands of phones in the country. Australia's criminals easily made up Phantom Secure's biggest set of customers.

The end result was a mountain of cash. A set of Phantom Secure shell companies used to collect proceeds from phones eventually pulled in $19 million. The distributor responsible then trickled more than $2.6 million to their personal account over a number of years. The lion's share went to an account maintained by Phantom Secure's CEO.

Best of all for the distributors, the business was completely legal. It wasn't a crime to sell an encrypted phone in Australia, even to a drug trafficker. Phantom Secure seemed completely immune to any police interference, and its sellers were getting rich. Ayik, who started this tidal wave of encrypted phones, made a fortune through the sales. And he pulled Australia's biker gangs and other criminals into the twenty-first century. The Comancheros had their guns and bikes. Now they had cryptography too.

Chapter 5

Ramos

Seated near the bar in the Richmond Cactus Club, a casual restaurant just south of Vancouver, Vincent Ramos, the soft-spoken CEO of Phantom Secure, caught up with a friend over lunch. With a pleasant and quiet demeanor, the businessman of Filipino descent did not jump out as someone who might be providing the technological backbone for organized criminals around the world.

The pair ordered. Ramos's friend, fellow businessman Walloce Sohl, who was in real estate, had a glass of red wine. Ramos didn't follow suit; he wasn't much of a drinker. This was one of the duo's sporadic lunches. Every now and then, Ramos would phone Sohl to ask about the real estate market, and the pair would then meet up to talk. He also revealed a secret: he suspected the authorities were looking into him and Phantom Secure. The cops were watching but had not arrested him.

Sohl, as he had done so before, asked when Ramos was going to give up this business. It was clearly a dicey area to be in.

"You should get out of it," Sohl told Ramos.

Ramos believed Phantom Secure was a legitimate business, even if its clients included criminals. He claimed he had already run the business by lawyers, he declared his income from the phones even when his customers paid in cash, and that an accountant then handled his taxes. He believed he wasn't doing anything illegal in Canada. Everything was aboveboard.

But in his conversations with Sohl, Ramos went further than the legal argument and touched on an ethical one. He compared himself to a gun dealer—it wasn't a vendor's responsibility what someone did with a gun

after buying one. Following that logic, he wasn't responsible if a criminal used his device for a drug trafficking operation.

Those criminals were up to all sorts of things. Importations of methamphetamine. Assassinations of specific people. Was he not responsible for that activity, even indirectly? Regardless of whether he saw a need to take ownership of such activity, Ramos did serve those gangsters.

After about ninety minutes, Sohl and Ramos finished their lunch. Ramos did not take his friend's advice. Phantom Secure wasn't going anywhere.

Sohl first met Ramos at a mechanic shop, years before he started Phantom Secure. Ramos was going door to door to different businesses trying to sell them satellite cards for watching pirated TV. Sohl was immediately impressed by Ramos's salesmanship. He bought a card. His real estate developer bought a card. Clearly, Ramos was good at this.

"What are you doing selling this shit? You should be doing better than that," Sohl told Ramos at the time. He certainly had the chops to sell more important, and expensive, merchandise. Ramos was also a salesman for the multilevel marketing company Amway. He upgraded to corporate sales for Canadian telecom giant Rogers and won employee of the month for selling phones.

"He was very business-savvy. His whole life, he was sales," a family member later recalled. Ramos was "a businessman to the core. Not a gangster in the slightest," someone who worked directly with him at Phantom Secure later said.

Ramos and Sohl kept in touch, and Ramos and his mother, a nurse, bought a condo from Sohl in another city near Vancouver. They paid the minimum possible down payment. For Ramos, this was just the first purchase of what he hoped would be many.

"When I make money, I'm gonna come and buy more stuff from you," Sohl recalled Ramos saying. That ever positive attitude was Ramos through and through. He later appeared in a video testimonial on YouTube for Allysian Sciences, a wellness and nutritional supplements brand.

Sohl became something of a mentor for Ramos. Ramos certainly respected Sohl's financial achievements; Sohl said he made multiple people millionaires through the real estate business and his pep talks. He recommended Ramos read more books, specifically ones that explained financial independence and building wealth. Sohl said that he can show people the how and the what of making money and investing. But each person needs to have a reason to do so—a why. For Sohl, that was showing his own family that he could still be successful without going to college. For Ramos, that was providing for his wife and ex-wife, Sohl believed. Ramos also had children with both.

Family and his relationships were a priority for Ramos. He coached his son's flag football team in Richmond and practiced jujitsu with one of his daughters. While making bracelets with his children, Ramos wore a Hello Kitty backpack. He was a good father, a good son, and a good friend.

Eventually, Ramos decided to ditch his job at Rogers and go out on his own. He told Sohl he was traveling down to Panama to launch a "network" and create some new company. On January 2, 2008, Ramos incorporated Phantom Secure Communications, Inc.

The office in Canada was staffed by four employees. Some of the staff were also of Filipino heritage and came to help Ramos run Phantom Secure. The vibe was professional, with accounting and everything you would expect. From the outside, Phantom Secure looked like an ordinary business. It many ways it was.

Ramos was not the tech guy; that responsibility fell to his partner. While Ramos was the CEO, this person was closer to something like a CTO. The CTO was a very difficult person who didn't mesh well with clients so Ramos kept them away from the end users. When a customer support team in India couldn't handle a client's issue, it was escalated to the CTO.

Initially Phantom Secure sold BlackBerries in the same way Ramos had sold Amway. The multilevel marketing giant became the template for his own company. Ramos hired distributors underneath him, who then either sold the phones themselves or employed their own agents to sell on their behalf. As the semipublic face of Phantom Secure, the money trickled up the pyramid back to Ramos. He still kept a low profile, but Ramos was the first salesman for the company. He continued to spend his time reading books on sales techniques.

Phantom Secure bought handsets from BlackBerry itself or from resellers and then stripped down the devices beyond recognition. Some of the changes were physical, with the device unable to take photos or make voice calls. The key change was the installation of software called Pretty Good Privacy (PGP). This coated emails in a layer of encryption that, ideally, only the intended recipient would be able to remove. Then they could read the email. If a third party managed to intercept the message—such as an internet service provider or a law enforcement agency—they would not be able to read the email's contents. While ordinary email was a message scribbled on an open postcard, PGP allowed messages to be posted inside an envelope.

Phantom Secure ran its email servers in countries such as Panama and Hong Kong, places that Ramos believed have a reputation as tax havens or for not providing information to authorities from the rest of the world. The company ran other servers designed to mask the physical location where its clients' emails pinged back and forth.

Phantom Secure's phones could only communicate with other Phantom Secure devices, unless the company made an exception and added a different firm's network to an allowlist. This wasn't even designed at first as a security benefit: It was a financial decision. It kept clients locked onto Phantom Secure and Phantom Secure alone. If users wanted to talk to their contacts, they had to persuade them to join Ramos's network too. Phantom Secure then charged their exorbitant fees; clients had no choice.

Phantom Secure projected an air of mystique and exclusivity with its product. The BlackBerry was already a sign of wealth or success in some communities at the time. Ramos took that and built an even more high roller brand on top of it. BBM, BlackBerry's proprietary messaging program, was hot when Ramos launched his company. Phantom Secure marketed itself as a step up from that, as the only fully privacy-focused solution available. The marketing worked.

Phantom Secure became a status symbol in Canadian nightclubs among VIP crowds. Businessmen, athletes, escorts. Real estate agents and accountants. The phones cost thousands of dollars for a six-month subscription, but to get the ball rolling, Phantom Secure discreetly gave phones for free to some of those VIPs. Early on, "questionable characters" bought the phones as well, one Phantom Secure seller recalled.

This was years before WhatsApp, eventually the most popular messaging program on the planet, fully turned on end-to-end encryption. Other encrypted messaging apps, such as Signal or Wickr, didn't even exist yet or were just emerging. So when Phantom Secure expanded internationally, it found its product in high demand. One distributor who had worked in a Toronto nightclub moved to Hong Kong and continued to sell the phones there. Hong Kong was a much more international city, with plenty of high-net-worth individuals based there and flying in and out. They were starving for a phone that would secure their secrets more than what was available on the ordinary consumer market.

"I literally just landed in Hong Kong and next thing you know it's like I'm the only water vendor in the Sahara Desert. It was wild, man," the distributor later recalled. Sales grew exponentially: clients included mainland Chinese businessmen who came to Hong Kong themselves or sent their assistants. Singaporean corporate executives too. The distributor also got clients in the United Arab Emirates and Russia.

Eventually, Ayik brought the phones to Australia and business exploded. Ramos saw the ABC News TV spot that linked Phantom Secure to an underworld assassination. He thought it was great marketing.

"This is the best verification on what we have been saying all along—proven and effective for now over 9 years," he wrote to one of his employees in a message. "It is the highest level of official authority confirming our effectiveness. It can't get better than that." Phantom Secure may not have targeted the Australian market—Ayik was the driving force there—but Ramos embraced it.

Ramos started to make serious money. He had a safety deposit box with a company in Beverly Hills that required some clients to scan their irises before accessing their valuables. Ramos stored cash and gold bars there. Phantom Secure also had bank accounts in Hong Kong, Singapore, Ireland, the US, Canada, and the Philippines. Phantom Secure swallowed some of that money in its exorbitant running costs. Ramos eventually paid over $200,000 a month just for the SIM cards that powered his phones. The servers then cost tens of thousands of dollars on top of that.

With this newfound wealth, Ramos put his children into private school. He bought more property, just like he said he would. Ramos passed down his generally balanced approach to finances to his employees and told them

to invest, not squander, their cash. Over all the years Sohl knew him, Ramos didn't change; he remained humble and didn't flash his cash much. He did make one reckless purchase: a Ferrari. He had never owned a sports car, and this was his chance. He admitted to Sohl that it was a stupid thing to buy. But he just had to.

This success made Ramos a figurehead in his local Filipino community. Here was a son of a nurse and a janitor who now ran his own business. "I'm probably one of the few that is successful," he told Sohl.

By the time of the Asia expansion it was already clear criminals were using Phantom Secure's phones. "We knew it was encrypted phones, and we knew there were probably some people who were getting it for more nefarious purposes," a family member said, referring to Ramos running an encrypted phone business. "It wasn't a secret."

In a way, Ramos was right, at least when it came to the legality of his business. It wasn't a crime to sell encrypted phones where Phantom Secure was based in Canada; it wasn't illegal to sell the devices to criminals in most of the rest of the world either. Law enforcement agencies couldn't do much to stop the flow of Phantom Secure phones, and they certainly couldn't plug the supply at its source.

Ramos was also right the authorities were looking into him. Back in San Diego, Young and the FBI probed for a way into Phantom Secure.

The San Diego team had made some progress since the Hanson arrest. Their initial plan was to spy on the Phantom Secure sellers in their own backyard. They were Gamboa, the seller who had inadvertently vetted the undercover FBI agent, and Christopher Poquiz, another distributor. The FBI took a member of Hanson's organization that had since flipped to the agents' side and used him to approach the pair of sellers.

In March 2016, the informant met Poquiz one morning to buy two Phantom Secure phones. Poquiz, in a black T-shirt and backward baseball cap, tightly held a bag while a surveillance camera pointed at him took a photo. The informant brought up the burgeoning encryption news of the

day: Law enforcement was attempting to break into iPhones. Apple refused to unlock an iPhone that belonged to one of the terrorists in the San Bernardino attack a few months earlier. Law enforcement agents had been able to extract information from older iPhones in some cases. The informant asked Poquiz, What about Phantom Secure? People were trying to do similar attacks on Phantom Secure's phones, Poquiz explained. If they did so, the phone would wipe itself after ten failed attempts.

The point of monitoring Gamboa and Poquiz, the FBI hoped, was to eventually slip an undercover agent into Phantom Secure as a fake seller. From there, the FBI wanted the undercover to work their way up the ladder to eventually land meetings and conversations with Ramos and his CTO partner. Perhaps the collected evidence could be used against Phantom Secure's resellers later too. The plan wasn't a bad one, but it was still early days and very much focused on smaller game: a couple of resellers in California.

The FBI had also prepared a trap for Phantom Secure when agents arrested the brothers behind the chocolate importation company. The plan was to have an informant send news of that arrest to Phantom Secure and request a wipe of the brothers' Phantom Secure phones. Then, the investigators would film the devices as Phantom Secure remotely deleted the data, catching them in the act of wiping evidence they knew was part of a criminal investigation. A clear obstruction of justice charge.

The informant, though, died of a drug overdose. The FBI's main door into Phantom Secure slammed shut. After that unfortunate death, the investigators were back to square one. The team decided to look beyond their own agencies for help. What about the other countries that had already been dealing with Phantom Secure phones for years? Young, Katz, and agents from the San Diego FBI took a flight to Sydney, Australia.

Chapter 6

Operation Safecracking

Around two dozen law enforcement officials piled into a government conference space in Sydney in September 2016. The officials from Australia and the US took their seats at a couple of tables in the room. Over the last several days, the Australian government, continually stymied by encrypted phones, had hosted a seminar of sorts focused on Phantom Secure. An alphabet soup of different agencies attended—the Australian Crime Commission, the Australian Federal Police (AFP), various Australian state police forces. The San Diego team traveled to Australia and first met with the New South Wales Police, since they had a relationship from the Hanson investigation. The officials' schedules were packed, with one-on-ones with individual agencies and then larger gatherings. This meeting, with all of the officials piled into the room, was the big one.

Representatives from each agency were to show the rest of the group what exactly they knew about Phantom Secure, and what progress they had made against the company or the phones. Then the coalition of officials would have a much better idea of how, or whether it was possible, to move together as one against Phantom Secure. Just after lunch, Young presented the San Diego team's findings to their foreign counterparts. The prosecutors and FBI had found that drug traffickers were using Phantom Secure phones. Phantom Secure would wipe clients' devices if they fell into law enforcement's hands. Agents had managed to get one of these phones and rummage through its messages. They had tried some other approaches but hadn't had a breakthrough yet.

After the San Diego team's presentation, the next agency stepped up. This agency's work was much more developed. The reality was that Australian, as well as Canadian, authorities had already been following Phantom Secure for years. The Americans were late to the party—their work looked like a fourth grader's in comparison, one attendee thought.

After the second agency's presentation, one of the FBI agents was first to speak. "Wow, okay," he said. "Do you guys need money or something?" Of course the American reaction was to throw money at the problem. Young even joked to the FBI agent, "Could you be any more American? Oh my god."

One of the FBI agents at the Australia meeting—not the one who made the money comment—was Nicholas Cheviron on the San Diego Organized Crime squad. If you searched Google Images for "FBI agent," the resulting stock images would probably look like Cheviron. His body mass index was exactly the requirement for what people thought an agent should look like; he had the quintessential short, neat, white guy haircut; and colleagues thought he was friendly without being memorable. He was also just really good at his job: Cheviron was focused on the work itself of doggedly investigating criminals.

He had been an FBI special agent for nearly ten years by this point. Before that, he was a police officer in Bloomington, Illinois, a city of around seventy thousand. From his more recent perch in San Diego on the border with Mexico, Cheviron ran informants, carried out physical surveillance, and snooped on criminals' messages. He had done it all in one of the hot zones of the drug trade. He was at the reins of the San Diego FBI's investigation into Phantom Secure.

Phantom Secure sold at least ten thousand phones around the world. Officials from some of the other agencies told Cheviron they were unaware of any law enforcement partner that had identified even a single legitimate Phantom Secure user. That suggested many, if not most, of these vendors were selling devices to criminals. Potentially ten thousand individual people who were probably part of crews like Hanson's.

The US authorities had already attended another meeting in May 2016 in Vancouver to coordinate with their Canadian counterparts. The point of that one was to figure out the scope of the Phantom Secure issue and what everyone knew about the company at the time. The Canadian authorities

showed they had made some headway too. Through March and August 2015, the year before, undercover agents from the RCMP successfully managed to buy Phantom Secure devices by posing as drug traffickers. This came after multiple failed attempts. At first the RCMP had tried to buy Phantom Secure phones through the company's website or by walking into its office while undercover. The RCMP tried this six separate times and encountered a formidable obstacle: Phantom Secure's vouch system.

When the RCMP agents finally did secure their phones, they fabricated the need to wipe a device.

RCMP: So, he picked up the load [of drugs] and I think he's been arrested and I need, there's a lot of evidence and fuckin' shit on my BlackBerry.
Phantom Secure: Yeah.
RCMP: I need that evidence gone, ASAP.
Phantom Secure: You wanna wipe both of them?
RCMP: Yes.
Phantom Secure: Okay then…
RCMP: Oh, you're a lifesaver.
Phantom Secure: One sec.
RCMP: And, but the thing is, cops can't access it, right?
Phantom Secure: They can't even access that anyways, yeah.

With that conversation, the RCMP had proof Phantom Secure's workers would wipe phones if told the purpose was to destroy evidence.

The Canadians, with Phantom Secure being based there, had the IP addresses of Phantom Secure's resellers when they logged in to the site used to manage their orders. This showed the approximate location of where these people were: Guangzhou and Beijing in China; Moscow, Russia; Aachen and Frankfurt, Germany; Istanbul, Turkey; Amsterdam, the Netherlands; Paris, France, and even back home in the US at the University of Michigan.

The Australian authorities, meanwhile, knew who sold Phantom Secure phones to criminals in different parts of their country. They would get names, mug shots, and more of at least eighteen people.

The San Diego team did not have all that much to provide in terms of intelligence. The Canadian and Australian officials were much further along with that side. What the US prosecutors could offer was perhaps more valuable: a novel legal approach that could be used to target Phantom Secure and take it down. The United States has a law called the Racketeer Influenced and Corrupt Organizations (RICO) Act. Prosecutors used it extensively in the 1970s specifically to target mafia bosses. These dons would rarely touch any drug shipments or carry out violent acts themselves, but there was still evidence that the crimes funded the organizations that carried out them out. RICO was designed to let prosecutors get the dons too.

The prosecutors in San Diego were also aggressive—they were willing to go out on a limb and prosecute cases as long as they could find some sort of link back to the city. Hanson's drug trafficking in San Diego was the link that allowed the prosecutors to now go after a Canadian company that sold its products to criminals in Australia.

The prosecutors had pushed charges under the RICO statute on Hanson. Now they could do the same to Ramos and his wider Phantom Secure organization. The key was proving that Phantom Secure was a criminal "enterprise" in and of itself. The prosecutors would need to get Ramos to admit he was selling phones specifically to facilitate crimes. That would be easier said than done—no one among the agencies appeared to have any ideas that could be turned into a real investigation. For all of the exchange of information, it seemed the meeting was ultimately fruitless.

Then right at the end of the meetings, two cops from Queensland, a state to the northeast of Australia, piped up after not saying anything for days. They said they had a guy, meaning an informant, under their thumb. This source was a Phantom Secure distributor in Australia.

Every big case needs a big break. Even if it seemingly appears out of thin air at the end of a multiday slog.

This, the agencies thought, could be their way in: rather than introducing an undercover to work their way up the ladder, they could get intelligence from someone who was already inside. Would the FBI want to take this person as a potential confidential human source (CHS)? That is, a mole inside Phantom Secure? The FBI did not hesitate. As soon as the agents got home to San Diego, they put the CHS to work.

Operation Safecracking, as the FBI called its Phantom Secure investigation, was a go. The San Diego team gave the case a logo that showed what they hoped to achieve: a sword piercing an email envelope icon.

Ramos was ready to sell some phones. Wearing a tight black T-shirt, he walked into a Las Vegas hotel room in February 2017 to meet with a handful of new "executives," what Ramos called his clients. David,[1] one of his highly trusted distributors, had arranged the meeting. The TV played a college basketball game in the background. The Duke Blue Devils were up against the North Carolina Tar Heels.

These five executives were from Southern California and Mexico, and they were interested in purchasing a whopping two hundred phones. Ramos took a seat on a sofa by the room's large windows and smiled as he ran the group through Phantom Secure's product. Quickly, the executives made their position clear: They were drug traffickers. Their group was looking for an encrypted messaging solution that would help their planned expansion in South America and Europe. Phantom Secure might be a perfect fit.

"Three of my main guys are in prison," one of the drug traffickers said.

"Mmhm," Ramos acknowledged.

"I lost, like, fifty kilos coming out from Colombia," the trafficker continued.

"Okay. You don't have to tell me that, but it's okay," Ramos replied.

"Yeah, well, we're all friends," the trafficker added.

"Just saying it out loud," Ramos said, tiptoeing the customers away from discussing their business with him so openly.

Ramos's own business was showing signs of stalling. Aggressive competitors shattered his monopoly on the Australian market. Rivals' products used Android, while Phantom Secure's phones were still on aging, and often busted-up, BlackBerry handsets. Even Ayik, one of Phantom Secure's biggest proponents, moved on from Phantom Secure. Along with

tech expert Afgoo, he pivoted to selling phones from another firm called Sky Global.

To a fault, Ramos still carried his positive attitude. He only wanted to hear good news from his resellers, even when some of them warned about encroaching competitors. David, the distributor who set up the Las Vegas meeting, was a breath of fresh air. Australians would never switch to the rivals, he told Ramos. People were loyal to the Phantom Secure brand. David said everything Ramos wanted to hear.

Ramos needed his business to survive to continue to fund his lifestyle and provide for his family. Some employees begged him to redeem Phantom Secure's reputation as a legitimate company. Instead, Ramos embraced the criminal market. He had chosen his customer demographic, and he leaned into it, hard. In the Vegas hotel room, Ramos continued to pitch the drug traffickers.

But they still needed something more to trust Ramos. The two parties were ultimately strangers to one another. How could they really know that Ramos and his company would be on board with using its phones for drug trafficking?

"You know, we don't know you," one of the traffickers said.

"Of course. That's what I'm saying. You don't know me," Ramos replied, now being much more vocal than in his previous answers. "But, yeah, that's exactly what I'm saying, right. We made it—we made it specifically for this too."

Ramos assuaged the traffickers' skepticism further by saying he was confident that Phantom Secure's phones could not be compromised. Through what he had heard, Ramos said, it was usually an informant that caused issues. That was the case "ninety-nine percent of the times," he said. If anything was going to be an issue, it would be the drug traffickers' own people and not their encrypted phones.

That led the conversation to a particular issue: if the traffickers did end up with an informant, they would want a way to pinpoint that person's location. Phantom Secure's phones ordinarily had the GPS functionality removed. But the traffickers wanted an extra feature: Could Ramos leave the GPS in, letting the smugglers track down a mole and kill them? Ramos stressed that a user would probably be able to just turn the tracking off. The smugglers kept pushing; they wanted to know the last location of one of

their workers in case a shipment came in and the employee's phone then turned off. One of the traffickers then imagined what they would say to their workers to make sure they kept the GPS tracking on.

"Yeah, don't fight—don't don't don't don't fuck with the phone. If you turn it off, we'll turn you off."

"Right, right, right, right," Ramos replied.

The traffickers also asked Ramos what he thought they should do if one of their people were arrested.

"What is it that you recommend? What's the first thing we should do if we get word that someone got pinched and we need to just kind of—have them fall off the radar?" one asked.

"You'd want, um, send a wipe command to his device," Ramos replied, flaunting Phantom Secure's signature feature. He then walked them through how that might fail if the phone were placed into a Faraday bag. That would stop the wipe in its tracks.

"Who has that?" a trafficker asked, referring to the Faraday bag.

"What I'm saying, the authorities, the 'unfriendlies' do," Ramos said.

Eventually he won the smugglers over. They didn't buy two hundred phones but instead agreed to purchase an initial ten Phantom Secure phones with a six-month subscription for $20,000.

Ramos left the meeting ready to please his new customers. Later he followed up with David to ask whether the drug traffickers were satisfied with the service. Ramos also said he was working to fix the GPS issue for the clients. After paying $20,000 for ten phones with six months of service, the traffickers renewed their subscriptions for another $25,000.

David was clearly good for Phantom Secure's business. He had brought in some very serious customers at a time when the company was desperate for more action. Ramos trusted him and promoted David's role inside Phantom Secure. This gave him direct access to the company's two major resellers who oversaw distribution in Australia, Hong Kong, Thailand, Dubai, and Turkey. Ramos wanted to put David in charge of all of Phantom Secure's Australian sales. Maybe he could give the Australian market the kick it needed.

David was not an ordinary phone seller. He was the confidential human source (CHS) that the Queensland Police Service in Australia had offered to the FBI back during the law enforcement meetings. After Sydney, the Americans had hosted a subsequent meeting in San Diego, with the Australians and Canadians flying over. Here, the agencies fleshed out how to leverage this informant.

David had secretly been a mole for much of the time Ramos knew him. And the drug traffickers he had met in Las Vegas and agreed to do business with: they were undercover agents in a joint operation between the FBI, the RCMP, and the Dutch authorities. They weren't there to expand their drug operations throughout South America and Europe. They were there to catch Ramos admitting he facilitated drug trafficking.

Those two secrets put a disastrous new context to everything Ramos had said in his face-to-face with the fake drug traffickers. Instead of growing Phantom Secure's business, Ramos had just signed its death warrant. Over the course of the meeting, Ramos had dug himself a deeper and deeper hole. He said Phantom Secure could remotely wipe phones of users the police had arrested. He discussed whether the company could use GPS technology to track workers' locations on the traffickers' behalf. He said Phantom Secure had made their technology "specifically for this" in a conversation all about smuggling drugs. All this flexing to the fake clients was very unlike Ramos. He was usually a serious guy when it came to business. He liked to party but not really show off. The threat to his Australian market share had changed Ramos, and this posturing may have just cost him his freedom. He had handed much of the investigators' case to them without even realizing it.

Blissfully unaware, Ramos continued to lean in to his criminal user base. In 2018 he traveled to Mexico City, where he secured some more clients. In a text message sent as he traveled back, Ramos told an associate he closed a deal with the Sinaloa drug cartel.

"We are fucking rich man," Ramos texted. "You better fucking appreciate it. get the fucking Range Rover brand new. Cuz I just closed a lot

of business. This week man. Sinaloa Cartel that's what's up and my boy is Punjabi Cartel lol."

Gone were the days of plausible deniability, of selling phones to criminals by happenstance. Ramos was knowingly in bed with dangerous and infamous drug traffickers, and he saw that as a reason to pop the champagne.

Footnote

1 Author has changed this person's name.

Chapter 7

Face-to-Face

Young and a half dozen or so agents crowded around a black-and-white TV in a dark Las Vegas hotel bedroom. The TV displayed a live camera feed into the next section of the eighteen-hundred-square-foot suite, complete with a granite wet bar, gaudy sitting area with couches and coffee table, and a breakfast nook. Tacky art hung from the walls. The suite was unapologetically Vegas.

It was a year after Ramos admitted everything to a gang of fake drug traffickers. Now, the FBI and its allies were to meet Ramos face-to-face. Beyond Young, the group of officials in the Wynn hotel included Cheviron from the FBI; another FBI agent and NFL fanatic Brett Fenoglio; Stephanie Stevens, a junior FBI special agent who became the subject matter expert on all things tech; and various AFP and RCMP agents. While Cheviron, Fenoglio, and two foreign agents waited in the lounge, the rest of the group waited in the bedroom. The room was not designed to house that many people, and some of the agents sat on the king-sized bed while they watched what was happening in the next room through the camera monitor.

At the moment, that wasn't much at all. Ramos, their hopeful guest, was hours late. He was supposed to show up to the room at two p.m. to meet David, the distributor turned informant. It was now late evening.

David had lured Ramos back to Vegas for this trap. While in the city this time, Ramos and David were set to watch a fight. Cyborg was up against Kunitskaya in a UFC tournament. Ramos's wife and one of their children also came along to the city.

Young and the agents believed they had enough evidence to lump Ramos under the umbrella of a RICO charge, potentially putting him behind bars for decades. The team could arrest Ramos as soon as he walked through the suite's door.

But they had another idea. The agents would corner Ramos and encourage him to give the authorities access to Phantom Secure using a tech method known as a backdoor—basically a way for third parties to read the content of messages. There was no telling how powerful that capability would be. If reading the contents of just one phone—Hanson's—had been a gold mine, what would it be like to read messages from thousands upon thousands of phones. That seed of an idea, planted when Young and Katz went through Hanson's Phantom Secure device, might now come to fruition.

Finally, Ramos was on his way. Agents got into position. Cheviron, Fenoglio, an AFP agent, and an RCMP agent readied themselves in the living room. Through the black-and-white monitor, the others watched as Ramos walked inside.

Immediately, one of the agents grabbed Ramos's Phantom Secure phone and handed it off to one of the AFP officials hiding in the bedroom. The group then searched Ramos for weapons and explained what was going on. Cheviron had pored over reports from financial investigators, bank records, and corporate filings. His conclusion was that Phantom Secure generated tens of millions of dollars of revenue as part of its business in selling encrypted communications to criminals.

On the other side of that hotel door, there were threats of a very long prison sentence. That was, unless Ramos put a backdoor into Phantom Secure. If Ramos did not agree and told the agents to pound sand, they were ready to arrest him.

Ramos, amped up, cycled through every excuse—I don't know what you're talking about; I haven't done anything wrong.

Back in the bedroom, Young sat on the bed with an AFP official who held Ramos's seized Phantom Secure phone. Miraculously, when an agent first swiped Ramos's phone and relayed it to others in the bedroom, the phone was open. No need to guess the password like the FBI had with Hanson's. This safe's door was left ajar.

Now holding that safe in his hands, the AFP official asked Young if he could look through the phone's contents. "No," came the blunt response. What do you mean I can't look through it? the official asked. We don't have permission, Young replied. The official asked what he was supposed to do then. Just keep it open, stop it from locking, but don't read anything.

"Are you serious?" the increasingly frustrated man asked. Young, deadpan, said he was completely serious. Do not look in the phone, Young reiterated, as he went on to explain US constitutional law, still in the dark, watching the black-and-white TV. The agents did not yet have a warrant, or Ramos's consent, to start mining that vein of intel.

After about two hours of back and forth between Ramos and the agents, Young came out of the bedroom to meet Ramos for the first time. He explained how much trouble Ramos was in, and the group showed him the undercover footage from a year earlier. That did the trick. Ramos was on his back foot now.

Eventually, after Ramos calmed down, the officials started a long conversation about what they wanted—the backdoor into Phantom Secure. The agents tried to convince Ramos to do what they said was "the right thing" for himself and asked if such a backdoor was possible.

That conversation went in circles for hours, and hours, and hours. At points Ramos would cooperate and offer up information. He worried that if he didn't, the agents would take him away before he could see his family. Ramos all but admitted to the FBI that criminal organizations were users of his company's phones. He also maintained that the company had legitimate customers too, but he didn't name any.

Then, he would pull back again. Ultimately, Young thought Ramos didn't trust the officials. That perhaps the FBI would get what it wanted, and then arrest Ramos anyway. That wasn't true, Young said.

For around three grueling days, this hotel suite became Ramos's and the agents' entire world. Agents slept in the suite alongside Ramos, while Young stayed in his own room. The group ordered in pizza, and a merry-go-round of officials came in and out of the bedroom, each with their own questions and taking turns to grill Ramos. The bedroom was like a clown car with more and more agents flooding out. Ramos asked how many people were even in it.

They showed him photos of other persons of interest connected to Phantom Secure and questioned Ramos's wife, who was staying in her own room nearby. In between the rounds of questions, Ramos was allowed to have breaks to see his wife and daughter. They thought he looked like a ghost.

Later on Ramos provided consent for the agents to access his multiple phones and laptop. The agents put Ramos's iPhone into airplane mode and snapped photos of messages, including the text where Ramos boasted of working with the Sinaloa drug cartel. Stevens, the junior FBI agent, stared at Ramos's laptop, day in and day out, keeping it open.

At one point after several days of questioning, Young told everyone, including Ramos, to get some sleep. They had finally made some progress: Ramos had agreed to come back to San Diego with the team. It seemed the agents might really get what they wanted.

Then in the middle of the night, Ramos got cold feet.

With the agents asleep, Ramos saw an opening. He got up and slinked out of the room. Ramos went to his wife's room and said his goodbyes. After navigating the hotel's boiler area and basement, Ramos emerged outside and made his way to a strip club where a friend was waiting. The pair got into a car and started the mad drive to the Canadian border, one thousand miles north of Vegas.

Ramos texted the agents and told them he just needed to go for a walk to clear his head. He was coming back, Ramos said. Back in the hotel, now awake and alert, the agents and Young tried to find where Ramos may have gone. They didn't want to go five-alarm fire just yet. There was a chance he would come back willingly. Other than that, they simply waited—if they were to get their backdoor, they didn't have much of a choice. The agents needed Ramos on their side.

But Ramos had no intention of returning. As he and his driver sped northbound on Interstate 5, Ramos used his associate's phone to message other Phantom Secure workers. He tried to warn them about what was happening but couldn't bring himself to say that Phantom Secure was dying. If he could just get across the border, and get to a lawyer, maybe he'd be able to put all of this behind him. Perhaps Phantom Secure would stay afloat.

Some people he spoke to couldn't tell if Ramos was being overly dramatic; they only realized later that Ramos, if anything, was underselling the gravity of the situation. The eternal optimist refused to accept the reality in front of him: this was the end. Ramos then said he was going offline. He shut down a Phantom Secure server that was going to facilitate the backdoor. He and an associate he was talking to wished each other the best, and Ramos went dark.

One of those people later said, "That was the last I heard from [Ramos]."

After Ramos shut down the server, the agents and Young realized he wasn't coming back. Ramos was on the run. Now, the team moved to Plan B. There would be no covert side of the operation. "We need to fire up the engines," Young said to Cheviron. "He could be alerting everybody."

If the authorities weren't going to get a backdoor, they were going to capture Ramos and shutter Phantom Secure instead. They went loud.

Agents alerted the airport in case Ramos attempted to take a flight out. Officials tried to pull CCTV footage that might give a clue as to where Ramos went. On his laptop, which Stevens had kept open, the agents were able to see what Wi-Fi networks Ramos's phone connected to. The first one, which appeared around eight hours after Ramos first took off, was simply "Starbucks."

"Well, that's a good clue," Young joked sarcastically. There could easily be a thousand Starbucks within an eight-hour drive of the hotel. The next Wi-Fi network to pop up was a Comfort Inn. "We literally called every Comfort Inn on the West Coast," Young later recalled. The group tried to dupe hotel staff into revealing whether or not Ramos was staying there by asking to be connected to his room. Some agents went to the Comfort Inns that were nearer by. None of it worked; Ramos was nowhere to be found.

In the suite, one of the agents came up to Young and told him about a new problem. In the search of Ramos's devices, the agents had come across

an alarming message. Someone, it wasn't clear who, had allegedly offered to sell Ramos information from the RCMP.

"You don't know me. I have information that I am confident you will find very valuable," one alleged message to Ramos read. The RCMP appeared to have a mole. In the hotel, in his thick French-Canadian accent, the agent told Young he couldn't tell for certain whether the person who allegedly offered this information to Ramos was not in the room right now. Nor whether that person had any role in Ramos's escape.

As if the embarrassment of letting their main suspect escape or the possibility of a mole weren't enough, soon the agents would lose their hotel rooms. A conference was about to be held at the hotel, meaning the group had to go home, no matter what, by Monday. They had spent the weekend buttering up Ramos, and now they all had to sleep in the same space. Two or three to a bed, the officials tried to get a night's sleep.

The morning after, the team headed to San Diego. On the way back, Young felt it was all over. The team had Phantom Secure nearly in their grasp, and then it slipped away. Once Young got back to his office, he swept items off the desk in frustration. There was no guarantee the investigators would ever get to this spot—of nearly backdooring an encrypted phone company—ever again. He thought, "This must be what it feels like to get to the Super Bowl and lose."

Chapter 8

The Capturing of Vincent Ramos

The usually drab US Attorney's Office turned into chaos. Katz and other staff had already been preparing for the possibility the FBI would need to arrest Ramos, at which point they would quickly file the necessary paperwork. With Ramos on the run, their plan changed from arrest to trace. Having heard of the escape, every prosecutor in the unit with a keyboard was conscripted to help. They had no idea where Ramos went. They needed to find him.

"It was all hands on deck," Katz recalled. Even people who had never touched the Phantom Secure case helped in various ways. The team scrambled: get on the phone; run to the courthouse; get this signed; prepare for the results. Customs and Border Protection and the US Marshals came into play to help locate and capture Ramos. Lots of frustrated waiting turned into hours of searching.

When authorities need to rapidly hunt down an escapee, there is also a ton of vital administrative work to get through as quickly as possible to ensure investigators have legal authorization to deploy certain tracking techniques. In some cases the prosecutors had to write up documents and then get judges to sign them, if the judges agreed with the authorities' argument that they needed this tool right now. On the data side, the authorities engaged with credit card companies to try to track Ramos's spending and see if he was using funds anywhere.

The team did have one lead when Stevens's constant monitoring of Ramos's devices finally paid off. A notification popped up asking if the user wanted to accept calls from a new phone. At first Young shrugged it off. It

was probably nothing, he said. Then someone else pointed out the number's significance: it was *Ramos's* new phone. He had switched. Now, the team had something to track Ramos with.

The team got judicial approval to pinpoint the location of Ramos's cell phone. A judge signed an order, which demanded the relevant telecom provide regular updates on the phone's approximate coordinates. As the pings came in every few minutes, they showed that Ramos was on Interstate 5. Six minutes later, the location was now farther north on the road. Then another, and Ramos was still barreling north, closer and closer to the border. It looked like Ramos was going to make it into Canada before agents on the ground could catch up with him.

This was nearly a worst-case scenario. Traditionally, fugitives flee to Mexico, where the process is relatively easier to haul them back to the US if authorities catch up with them. But a Canadian citizen, getting back to Canada, who wasn't actually guilty of a crime in Canada, was a much more complicated issue. Even with Canada's very close relationship with the US, it could take years for Ramos's home country to extradite him, if at all. It would be easier for the investigators if Ramos were driving the opposite way down Interstate 5 and fleeing to Mexico instead.

Once Ramos arrived at the border, he would have a few options. The final stretch of road before the crossing lies alongside the Peace Arch Historical State Park, whose namesake, a sixty-seven-foot-high arch, sits on the boundary of the two countries. Ramos didn't even need his driver to take him through the border crossing for vehicles, where an official might catch him. Ramos could, if he liked, symbolically run through the marble arch itself to his freedom, although he would probably be spotted.

Or, he could take a comically easy approach. Around five hundred feet to the right of the arch and across the main road was a small playground, with a brown swing set and sky-blue picnic benches. The length of the playground to Canadian soil was just over 160 feet, a casual sprint or quick walk from the nearby parking lot. There wasn't even a fence, just a small ditch with a convenient footpath so people could simply walk over the border. For Ramos it would technically be an illegal border crossing, but he would be home, and out of the reach of his US pursuers.

But he wasn't there yet. The pings from Ramos's phone stopped before he reached the border. Whoever was driving Ramos up to Canada

seemingly wasn't prepared to actually take him the final leg across the immigration checkpoint. And Ramos wasn't taking the route through the park's playground either. Instead, the pings showed him more than twenty miles south of the border in Bellingham, a small city of about ninety thousand people.

"Call everybody," Cheviron told Young in a phone call when Ramos arrived in Bellingham. Young and the other prosecutors alerted everyone they could in the area, Googling nearby sheriff's departments.

Then, the pings stopped moving altogether. Ramos was in a particular spot: a breakfast cafe in the same shopping plaza as a Trader Joe's. This was the investigators' chance.

On the run, Ramos needed something to eat. In blue jeans, a ripped gray hoodie, olive-green waterproof jacket, and black-and-white Nikes, Ramos entered the Over Easy cafe at around 12:30 p.m. He took a spot with his back to the wall. This gave him a wide view of the rest of the cafe and whoever might come inside.

Ramos managed to experience a moment of normalcy after his surreal days in the Vegas hotel room. He ordered some food as the few other patrons of the cafe ate too. The cafe wasn't busy; this was the time of day where things really slowed down. To the cafe owner, Ramos looked like a big gentle bear.

Two men then entered the restaurant and came to the bar area. They stood there and appeared nervous, almost hyper. They looked back outside the cafe and seemed distracted, as if they were waiting for someone.

"Hey, do you guys want to order something?" Jamie Bohnett, the cafe owner, asked the pair.

"We're not quite ready yet," one replied.

Suddenly, the two men were joined by three or four others. They walked toward Ramos.

Ramos didn't resist. One put a hand on Ramos's shoulder and escorted him out of the cafe. No yelling or shouting, no guns drawn. The dramatic

manhunt had come to an end in as quiet a manner as you could imagine.

"Well, I guess we're done," said one of the officers. Ramos got into the cop car, hunched forward, and stared straight ahead.

In San Diego, a member of the team yelled down the sixth-floor hallway, "We got him!" High fives rang out through the office.

Arresting Ramos was just one part of the overt strategy. Sohl said agents searched Ramos's family home and found cash bundles wrapped with the Phantom Secure logo. On the other side of the planet, Australian authorities executed over a dozen search warrants in which they seized more than a thousand devices.

Most significantly of all, the FBI and its partners shut down the Phantom Secure network itself. They took control of more than 150 web domains used by Phantom Secure as part of its infrastructure. Law enforcement agencies in Hong Kong and Panama, where Phantom Secure positioned its servers specifically to stay out of the hands of police, assisted too.

The Sinaloa drug cartel in Mexico, biker gangs in Australia, and thousands of other criminals lost their communication lifeline to one another. Their Phantom Secure phones, and the technological backbone of their drug smuggling empires, went offline.

The investigators plastered the emblems of the FBI, the AFP, and the RCMP across Phantom Secure's website. A small text box sat at the bottom of the page, where Phantom Secure users could enter their email address to check if they had been swept up in the investigation. Anyone entering their personal information into the site was of course potentially giving that straight to the authorities.

The FBI didn't manage to get its backdoor, but they did shut the company down. With that, the FBI still telegraphed something to other companies in the wider encrypted phone industry: we will come after you. The gold rush of selling encrypted phones to crime rings appeared to be over.

Dressed in a khaki prison jumpsuit, Ramos was in front of Judge William Hayes in a San Diego district courtroom at just past ten a.m. in late May 2019. A mass of Ramos's family came down to San Diego for the hearing: In the back row of benches were Ramos's wife, sister, brother, and sister-in-law. His mother was also there. Ramos's father was back at the hotel looking after Ramos's six-, eight-, and ten-year-old children. His wife had only been able to come see Ramos a few times since his initial arrest in the Over Easy cafe more than a year earlier. It wasn't easy to find the funds to travel to San Diego after the authorities seized Ramos's assets. The US had let Ramos's wife keep some money from the sale of a house, but that money would run out fast.

Young and Katz were in the courtroom too, ready to argue on behalf of the government on what length of time it thought Ramos should be behind bars. Young would finally get to perform in a courtroom once again.

Victor Sherman, Ramos's lawyer, started the proceedings with a plea to the judge for leniency. The idea that Ramos wouldn't be able to have a real relationship with his children for as much as a decade seemed unbearable. By the time Ramos got out of jail, he might be in his early fifties. They were going to grow up without him. On top of that, his parents were now eighty and eighty-five years old, and not in the best of health. There was a good chance they would pass while he was locked up, an excruciating fact for Ramos. Sherman asked the judge to weigh Ramos's anguish as he set a sentence.

Sherman then moved on to something he and Young agreed on: Ramos was the first person prosecuted by the US for running an encrypted phone company. The much earlier prosecution of Nat Lineham, who ran Phantom Secure's predecessor beStealth, had been based around a drug crime. In Ramos's case, the US was arguing that Phantom Secure was a criminal entity in its own right.

This was uncharted territory. That lack of legal precedent over his business was one reason Ramos went as far as he did. "I am not dealing with these drug dealers; they are one or two steps away from me; I am

selling a phone; I am in a business," Sherman said in the courtroom of his client's thinking to his lawyer. There was no clear rule that selling these phones to drug traffickers was even a crime. How could Ramos possibly know he was breaking the law? He was the first person ever to be prosecuted in the US for it. The attorneys in the courtroom understood it was illegal to sell a phone if you know it is being used for an illegal purpose. That would fall under conspiracy laws. But lawyers knew the law better than most people. And Ramos was not a lawyer.

Sherman asked the judge to give Ramos a roughly eight-year sentence and hoped Ramos could transfer to a Canadian prison to be closer to his family during part of that jail time.

After hearing Sherman's argument, Judge Hayes immediately turned to Ramos. Hayes asked if the defendant wanted to say anything.

"Yeah, good morning, Your Honorable Hayes," Ramos started. He apologized to the court, the government, and his family. He especially thanked his wife. "I love and appreciate you.

"I deeply regret and I am remorseful for my actions and negligence that allowed my company to grow the way that it did. I made mistakes and decisions that I cannot take back. I should have acted more responsibly," he continued.

In October 2018, Ramos agreed to a plea agreement as part of his racketeering conspiracy admission. As part of the guilty plea, he agreed to forfeit $80 million to the US government, which is what the authorities calculated was Phantom Secure's net proceeds during a certain period.

Ramos admitted that he essentially knew his customers were criminals. He wrote in an earlier letter to Hayes that "I would be lying if I said that I wasn't aware of what was going on.… The reality was that I turned a blind eye and didn't want to face reality. I was making money and providing for my wife and children."

Now lumped in the San Diego courtroom, Ramos apologized directly to the judge for how he ran Phantom Secure.

"As I stand here in your courtroom today with my fate and future in your hands, I ask and hope for your leniency when making your decision when imposing your sentence. I am truly sorry, Your Honor. Thank you."

Young's turn to speak was next. He focused on the nature of Ramos's misdeeds.

“The scope of this crime, Your Honor, is staggering,” he said. Young said Ramos’s own estimate for how many Phantom Secure users were on his network was seven thousand. The US, Canadian, and Australian authorities had not identified a single legitimate user among those. In other words, Ramos might have been serving up to seven thousand criminals—seven thousand individual people involved in schemes like drug trafficking and murder from across the world. Hanson’s crew of six to seven people used Phantom Secure to smuggle a massive amount of narcotics from Mexico to Canada and Australia. Multiply that activity by at least a thousand, and you had the breadth of Phantom Secure. Ramos was the one who facilitated that gargantuan amount of crime.

“We’re talking about levels of drug trafficking that are just probably not even contemplated by the sentencing guidelines because they are so staggering, so high,” Young said.

Ramos may not have been aware of murder plots carried across his network, but he certainly knew about the drug trafficking, Young argued. And the purpose of the company, demonstrated through hosting its servers in Hong Kong and Panama, using code words for their customers like “executive,” and wiping devices it knew were seized by the cops, was to prevent law enforcement from investigating crimes.

For some, it was controversial for the FBI to shut down a company that was providing a secure communications service. Ramos did not deal drugs himself. He sold a technology that could be used for good or for bad. Ramos said privacy advocates, attorneys, and others wrote to him while he was in prison awaiting sentencing to criticize the case against him. What was the difference between Ramos and Tim Cook from Apple, or Sundar Pichai from Google and Alphabet? Both of those tech giants’ customers inevitably included criminals.

Young had a rebuttal.

Ramos “was not prosecuted because he was selling encrypted communications and encrypted devices to criminals. He was prosecuted because he was in agreement with these people, providing them the technology that they could use to facilitate their crimes, and the criminals that are spilling into this industry are the most sophisticated in the world,” Young continued. “These are not on the street. They are not using burner phones. These are some of the most sophisticated criminals in the world

using some of the most sophisticated technology in the world to hide from law enforcement." He asked the judge to put Ramos in prison for fourteen years, nearly double what his defense team hoped for.

Judge Hayes summed up the man in front of him. As with many individuals he had sentenced, Ramos's history and characteristics were mixed. The judge said Ramos was a gentleman and a very talented businessman who was successful in his legitimate employment before he created Phantom Secure. But Ramos changed, and served criminals.

Judge Hayes prepared to hand Ramos his fate.

"I am going to impose a sentence of 108 months," Judge Hayes said. "It is significantly less than what the government is requesting. The government is requesting a sentence of 168 months. This is five years less than that." The judge didn't think Ramos was in the same category as Owen Hanson, whom Hayes earlier had sentenced to more than twenty-one years in prison. The sentence was still more than what the defense wanted. Plenty of other people who came through court had made quick, dumb choices: eighteen- or nineteen-year-olds who decided to drive some drugs for $3,000. Ramos was not that.

"He is a smart gentleman, and I think he understood what he was doing. He took a risk, and it didn't work out very well at the end," Hayes said. "But he has also accepted responsibility. He's done everything that he can to put himself in the best light possible." As well as his lengthy prison sentence, Hayes added a requirement to Ramos's eventual three-year period of supervised release: he must not develop or maintain encryption services or devices. The only other thing Sherman asked for was that Ramos be incarcerated at FCI Sheridan, the prison closest to western Canada.

Judge Hayes concluded the hearing by speaking directly to Ramos. "All right. Good luck to you. Thank you." With the strike of the gavel, the CEO of Phantom Secure was ushered out of the courtroom and into prison.

Chapter 9

Vacuum

Ramos's conviction made two things clear: The San Diego team now knew it could target other similar companies, those that still sold encrypted phones to organized crime. And the owners of those companies realized they might be next. Clearly, the FBI knew about this industry and was not afraid to spend serious investigative resources to hunt, infiltrate, and ultimately shut down its biggest players. The authorities would also put their founders in prison. High-security phones had been lucrative for a time, but that period was over. The San Diego team wasted no time in opening a file on another massively popular encrypted phone firm: Sky.

While making his argument in the San Diego courtroom, Young had said people around the world were watching the sentencing. That included those who made cryptocurrencies that criminals used, members of the dark web where people sold all manner of items online, and other individuals who ran encrypted phone companies like Ramos had.

"They are watching what happens here today. They are watching the sentencing. And they are making decisions based on whether or not they are going to continue to provide these products and technology to criminals and whether it is worth the risk," Young said at the time.

Those people certainly were watching. One was Jean-François Eap, the CEO of Sky. Eap, it seemed, could easily be the next Ramos.

Eap's story was eerily similar to Ramos's. He operated Sky out of Vancouver, Canada, the same country as Phantom Secure. Eap also worked for a telephone and internet provider that partnered with Rogers, just like Ramos worked for the telecom giant before creating his own business. And

Eap started the company with good intentions before it transformed into something else.

"We all wanted to make a great product. And we all thought about what bad people might do with the phones. But… we had ideals to help privacy in the world," a former Sky employee said.

Eap ran Sky like a normal small tech company, with a culture of encouragement and teamwork. Developers transparently listed their work for Sky on their LinkedIn profiles. Its website included smiling illustrations of its various senior staff, as well as a doodle of Leo and Evee, the office Klee Kai and Shiba Inu dogs who held the title of Directors of Animal Resources. Despite the cutesy marketing, Sky had a clear reputation as being one of the few other encrypted phone companies that were popular among members of organized crime.

"We knew bad people used our tech. Just like bad people use Signal or WhatsApp," one former employee later recalled. The difference between those apps and Sky was that Signal and WhatsApp were both free to download and widely used by members of the public. Sky, meanwhile, sold premium-priced phones, which authorities said eventually ended up in the hands of many organized criminals. There were no two ways about it: whether Sky intended to or not, its products were the device of choice for certain sectors of drug traffickers.

One of the issues was unauthorized resellers. In many instances, they sold Sky's phones under pseudonyms. Phone sellers who already had Rolodexes of clients simply became Sky resellers and sold the devices to their customer base. Law enforcement said at the end of many of those resale transactions was a gangster. And some of those resellers did cater specifically to criminals.

After US authorities opened their file on Sky, they managed to catch Thomas Herdman, an international distributor of Sky phones, allegedly talking about how the product could be used to facilitate drug trafficking. The government's evidence against Herdman was some of the best an investigator could hope for. In one alleged conversation, when someone asked Herdman if it was possible to use Sky devices to organize international cocaine shipments, Herdman essentially repeated back to the person, yes, you can use these phones to organize international cocaine shipments. Herdman also allegedly went on to discuss destroying evidence.

In the wake of Ramos's arrest, Sky moved to get criminals off its platform. Sky trawled the internet for advertisements of Sky phones. It found dozens of resellers brazenly selling the phones on Instagram, Facebook, and eBay, some of whom explicitly said the phones could be used for crime. On social media, unauthorized people selling Sky devices created their own websites, put up classified ads on sites like Gumtree, and undercut each other's prices. Resellers were out of control.

Sky employees went undercover to figure out what these resellers were doing. They posed as interested customers and sent messages to the seller accounts. It was like when a company may hire a mystery shopper to go into their store and check whether their customer service is up to snuff. Only for Sky, it was to determine if their resellers were helping facilitate drug trafficking and, if so, to cut them off.

Encrochat, another phone firm highly popular among crooks, went in the opposite direction from Sky. Instead of hiring lawyers and cleaning up its act, Encrochat went underground. So did a number of other smaller providers. It was better if people didn't even know they existed while they continued to spread phones among organized crime groups. No websites. Unincorporated. Dark.

Ramos may have been the head of Phantom Secure, but he wasn't a one-man army. After the arrest of their CEO, distributors who worked for the company realized they were targets too. Concerned they would be grabbed by the FBI, they went on the run. One tried to buy a fake passport and ended up staying in low-budget hotels in city after city to remain under the radar. A bank froze his accounts, including one that contained over a million dollars. As long as he was free, he had not lost, he told an associate. He was "staying off the grid" and suggested Dubai as a potential safe haven.

Afgoo, the Phantom Secure seller who first approved the phones for Hakan Ayik, had another plan. He had been laying the foundation for his own encrypted phone company while also working for Ramos. He poured his own money into the pet project.

Having been in the encrypted phone industry for years, Afgoo was very technically minded, able to understand the minutiae of particular encryption algorithms and why one was better than another. But Afgoo wasn't much of a coder; he was more of an ideas and business guy with a geeky slant. Ayik was pure bravado; Afgoo made his sales pitches sound specific and credible. Together, they pushed both Phantom Secure and Sky phones throughout the world. Ayik got rich, again, from the phone business, run in parallel to his drug trafficking empire.

The FBI's shutdown of Phantom Secure ensured that its users became isolated, unable to contact one another through the secure channel they had been using for years. Downtime in a criminal enterprise costs money, and criminals needed a new encrypted phone, fast. Now with the understanding the FBI was finally coming after encrypted phone companies and their workers, Afgoo saw an opportunity.

Just a day or two after Ramos was caught, Young got a voicemail from Afgoo's attorney. He was headed to the US. Once the attorney landed and met with Young and the team in San Diego, he offered a menu of different items that Afgoo could help with. One of those was Afgoo's in-development phone, Anom. In a pitch that could have been a Silicon Valley PR event, the lawyer made the case that Anom was going to be the next generation of encrypted phone. Afgoo had already poured a substantial amount of his own money into Anom's development and had planned it to be a successor to Phantom Secure. All the infrastructure for the phone network was ready to go.

Afgoo, through his lawyer, was in effect making an extraordinary offer: Would the FBI like to use Anom in its own investigations? Would the FBI like to control Anom? In exchange for the possibility of a reduced sentence related to charges he was facing, that is.

The potential for Young, Cheviron, and Stevens, who would all go on to lead this project, was staggering. After all this time, and the disappointment of not being able to get a backdoor in Phantom Secure, a potentially even better prospect had fallen into their laps. They wouldn't seek to push a backdoor into an existing service. They would simply run the backdoored encrypted phone company themselves. Rather than painstakingly investigating an encrypted phone firm and trying to shut it down, the team could do it the other way around. They could instead manage a company,

and in their privileged position as the secret owners, read the users' messages.

The FBI and the San Diego prosecutors could keep their momentum from the shutdown of Phantom Secure going. Phantom Secure's now former customers needed a new phone company to launder their secrets, and Anom could fill that void, with the users having no idea that they were migrating into a trap. This was a new, daunting stage in the FBI's targeting of organized crime. Nothing quite like this had ever been done before.

In an extra audacious part of the plan, what if law enforcement knocked out Anom's competition in the secure phone industry? If the FBI closed down Sky entirely, like it had with Phantom Secure, those customers wouldn't just call it quits and go home. They would find a new provider. Lying in wait to happily take on those clients would be Anom. The criminals would flee from one company straight into the FBI's own, where they could be spied on. The authorities could make Anom even bigger.

"Everybody recognized as these other companies went down, those customers have to go somewhere, and we want to be positioned to absorb them," Young recalled. If the FBI secretly ran its own company, and later revealed it had been behind Anom all along, that would shatter the trust any criminal had in the industry. The FBI could fundamentally undermine the underground encrypted phone industry as a whole. What was to say that any other new companies weren't also managed by the authorities?

Soon, Young was on a plane to meet Afgoo in a secret location overseas. Heat, sounds, and smells overwhelmed Young as he navigated densely populated streets. The first to arrive in the country before the FBI agents, Young tried to find brief refuge in an Irish pub.

Young, Cheviron, Fenoglio, a DEA agent, and some AFP officials met Afgoo in a hotel suite. The vibe was immediately more relaxed than it had been with Ramos in Vegas. The agents were excited. Here was a person not only willing to collaborate but going out of their way to do so by offering up Anom first. With Ramos, the FBI and Young tried to convince him to put

in the backdoor. With Afgoo, he was trying to prove to Young and the FBI that he had something of value.

Being in a room with a herd of agents, initially Afgoo was pretty guarded. Young built a rapport with him. The pair bantered about sports—American football was the best sport in the world, obviously, and Afgoo became friendly. Much of the time, Afgoo sat in the corner of the suite with an AFP tech liaison known as CIN325. CIN325 was tasked with figuring out whether a backdoor into Anom was actually possible. In that suite, Afgoo and CIN325 geeked out over the details.

One morning at four a.m., Young sat on the side of his bed in the pitch dark and mapped out how it might be possible for the US authorities to secretly control Anom. Young then joined the FBI agents for breakfast in the hotel—one of the agents was big on hotel points. Over that basically free food, Young told the agents they should take a shot at running Anom. "Let's go for it. Let's just go for it until somebody tells us to stop," he said.

When the Americans told the AFP agents they wanted to go ahead, the AFP looked like kids on Christmas morning. The plan was to have the Australians try out an Anom backdoor first. Young believed the US government wouldn't get behind the idea without first knowing that it would work. The AFP and its grinning agents were fine with that—they probably wanted the backdoor more than anyone, Young thought.

While the group continued to meet in the suite, at a bar Young and another of Afgoo's attorneys hashed out what a cooperation agreement would look like.

"Look, I'm not going to have another Ramos on my hands, where he burns us," Young conveyed to Afgoo's lawyer at one point.

Later, an agreement was made: The FBI would pay Afgoo $120,000 plus nearly $60,000 in living and travel expenses, and the government would seek a reduced sentence if the authorities decided to prosecute him. In return, the FBI would get their backdoor.

All week long, the team worked fourteen hours a day on how to make Anom work. From the moment they woke up to when they went to bed, Young and the others discussed technologically how to do it, legally how to do it, operationally and logistically how to do it. Often this planning was in the hotel rooms. In the evenings, Young and the FBI and AFP agents went out for food and drinks and discussed next steps. One night, the group

bought two bottles of grocery store whiskey and passed the drink around, feet dipped into the hotel hot tub.

To some the idea still seemed crazy. The FBI did not know how to run any tech company, never mind one specifically for criminal customers. The San Diego team did have some comparisons to draw on, though. Investigating Phantom Secure now meant they had seen what a successful encrypted phone company looked like. It had customer service. A system of distributors who only let in certain people so clients could know their business partners, and the phone company itself, were trustworthy. Useful gizmos that clients wanted like the remote wipe. The FBI could disrupt the phone industry with even more new, exciting features, and get criminals to jump to their platform. If the investigators were going to flip Anom to their own needs, they needed all of this at a bare minimum. "We can't just run a good investigation; we have to run a good company," Young said.

The FBI would also, technically, be breaking the law with some parts of the investigation unless they received approval. Handling money from Anom sales that the FBI knew were the proceeds of drug sales would be money laundering. They would require covert bank accounts that couldn't be traced back to the agency so as to not blow the operation. The FBI would then have to lie to the banks about why they were setting up these new accounts; that was also a crime—fraud. That was standard behavior in a covert investigation, but, still, Anom was not your normal undercover operation. The amount of money coming in and out could be massive.

The stakes would be nail-bitingly high. If top-tier drug traffickers found out Afgoo was secretly providing Anom customer messages to the FBI, his life would almost certainly be in danger. People are killed in the criminal underworld over twenty thousand dollars. What would they do to someone who gave the FBI a backdoor to the underworld's most important form of communication?

There would be some incredible hurdles. How would the FBI and the AFP even get the Anom phones into the hands of criminals? Anom was still a tiny startup at this point, more Afgoo's brainchild than a functioning company. It didn't have much of a customer base yet, and the FBI would need to find a way to fix that. Would law enforcement sell the phones itself, or let them spread organically through encrypted phone resellers?

How would the FBI tread the very fine line of acting on any intelligence it managed to gather from the platform, while not making it obvious to Anom's expected criminal users that their phones were secretly bugged? If any one of Anom's customers found out, they would ditch Anom in an instant and likely warn their co-conspirators, severing the authorities' visibility and destroying the whole operation.

Analyzing the intelligence presented issues too. How would the investigators identify who was who on the platform? That was a common problem with listening in on suspects' calls, but with Anom, it had the potential to grow to a size that dwarfed even some of the largest wiretapping operations.

And the endeavor would be expensive. Encrypted phone companies have to source their hardware—the actual Android phones in this case—from a supplier. Then they have to pay developers to continually improve upon the software. Firms have to rent servers to route messages and keep them constantly online to appease their customer base. The FBI would need to pick up the bill for a lot of this.

No one would actually use Anom if it were an inferior product. They had to be just as good as the criminal organizations that were behind other secure devices; ideally, they would be even better than them to attract the more prestigious customers.

But despite all this, the proposition was incredibly tempting. If the agents pulled it off, the amount of intelligence from Anom could be enormous. After years of being stymied by encrypted phones and being unable to intercept criminals' communications, Anom could be the AFP's breakthrough for dismantling biker gangs and trafficking groups. For the FBI, it could be their window into countless more people like Hanson. As an incredible cherry on top, Afgoo still harbored connections to Ayik, the drug trafficker who had long evaded Australian authorities. If Ayik picked up an Anom phone, that could be a way to finally track him down.

The tool that syndicates had used for years could be turned against them. The team could identify the El Jefes of the world: The smart criminals, the ones who usually never appear on law enforcement's radar. The ones who believed they were untouchable because they were. Until now.

The evening after Young told the AFP the plan was to go ahead, the team went to a restaurant. This place was more upmarket than the corner store

food they had gotten used to over the last week. There, one member took a photo, a memento capturing the day the authorities decided to run their own encrypted phone company.

On the plane back to San Diego, Young pondered whether Afgoo might flake on the team and disappear. He wondered how much of the past week might have just been Afgoo sizing up the authorities, to determine how much of a threat they really were.

Afgoo seemed on board. But on a technical level, the FBI still needed to know whether a backdoor would actually work. They needed reassurance that Afgoo wasn't making an empty promise. The FBI and their colleagues in the AFP needed more proof.

Act II

Chapter 10

Anom

Athit[1] started his workday at 9:30 a.m., like he almost always did in late 2018 at his new coding job for Anom, with his MacBook on his chest while he lay in bed. Sometimes he sat up and had the laptop in front of him on the sheets while he fixed bugs in the company's Android app. Athit's real desk in another room was mostly reserved for video meetings over Skype with the rest of his team and when Athit had to look more presentable. He did the vast majority of his job, until six p.m., from the same spot he woke up in, inside his family's house in an Asian country.

That home, built by his parents, was a peaceful environment to code in. Athit and his wife lived on the third floor, while his parents lived on the second. Outside was noisier, as people milled down a dusty road next to long rows of shacks with corrugated metal roofs. Market stalls served snacks next to stray dogs.

At around ten a.m. he eventually rolled out of the bed to put together some breakfast. Then Athit made some coffee—he never went out to coffee shops—and after eating for ten or fifteen minutes, returned straight back to his makeshift office among the pillows.

Athit worked on Android apps for clients, and before contracting full time for Anom, he jumped from project to project. His portfolio included a calculator app, another that tracked when users fed their baby, and a third that increased the power of the users' phone speaker. It was not particularly exciting, or stable, work. He found a lot of these short-term gigs through freelancer websites like Upwork.

One day Athit was scrolling another of these sites called Angel.co, when he came across a listing for a full-time job. The listing didn't say what the specific project was that successful applicants would work on, and the company was one registered in Dubai that Athit had never heard of. All the listing divulged was that it was a job involving encryption and secure technologies. Still, it looked like a good opportunity. After living gig to gig Athit was ready to join a startup and be part of a team. Most importantly for Athit, the job was remote so he could continue to work from bed.

After applying, Athit had a video interview with the company's project manager, a hip, bespectacled man who lived in Bangalore, India. Athit believed he did well with the questions. The firm already had around a half dozen members on the development team, the manager explained, and the work was specifically on an encrypted messaging app called Anom. Athit was on board.

By now ordinary consumers, businesses, and governments had a healthy appetite for apps that sent secure messages. The world's citizens had been shaken by the revelations of former NSA subcontractor Edward Snowden years earlier. Snowden's leak of a mountain of classified material to an initially select group of journalists revealed that the US government performed mass surveillance of its own citizens. Some of the country's allies carried out similar levels of bulk monitoring by tapping the undersea cables that nearly instantaneously ferry data from continent to continent. The NSA also specifically targeted the network connectors of tech giants like Google and Yahoo and pinpointed the moment those companies stripped their users' messages of encryption. That's where the NSA inserted itself to then hoover up reams of peoples' email data and metadata.

The need for widespread encryption became much more urgent, and Snowden's leaks were a powerful catalyst for tech companies to finally take encryption more seriously. WhatsApp, the most ubiquitous chat app in the world, fully turned on end-to-end encryption for its then hundreds of millions of users (WhatsApp later grew to two billion users, all of whom had the encryption turned on by default). Smaller firms and organizations stepped up to the task too. Encrypting connections to your website became the norm for administrators all over after a nonprofit called Let's Encrypt released tooling that made the process much simpler and, more importantly, free.

That idea of anyone being able to enjoy the benefits of encryption without paying or needing a brain filled with technical knowledge became a tenet for modern-day privacy advocates. The same year Athit started his job at Anom, the cofounder of WhatsApp helped launch the Signal Foundation. This was a nonprofit that would take part in overseeing the continued development of Signal, an increasingly popular app and the gold standard in robust, and easy to use, secure messaging. A dizzying number of apps and software at various points entered the fray, with varying levels of security and success—Telegram, Threema, Wickr, Ricochet, and countless others. The Anom developers used one of these myriad apps, called Wire, to coordinate among themselves.

Alongside the boom in free-to-use apps for ordinary consumers, corporations and government agencies wanted encrypted messaging too. Any business could overnight become a hacking target. Having access to a reliable encrypted messaging program certainly wasn't a real defense against hackers; it wasn't designed for that. But such an app could hopefully provide a secure, digital war room where employees and executives could gather when figuring out how to respond to such an attack. Businesses also wanted to protect their sensitive communications from prying governments, be those domestic or overseas.

A lot of businesses and government agencies had an extra requirement of these messaging apps that normal users did not: they needed a way to archive the texts their employees sent to one another. For corporations, this might be to comply with the law if they were in a heavily regulated industry such as finance. Encrypted messages that couldn't later be descrambled in the course of an insider trading investigation, for example, would cause a blind spot. Government agencies had their own recordkeeping laws to contend with, and archiving messages allowed them to investigate abuse among their ranks.

One of the many encrypted messaging apps on the market had solved, and made tens of millions of dollars from, this problem. San Francisco–based Wickr started in 2012 as a privacy-championing startup. Its blond, straight-haired founder Nico Sell religiously wore sunglasses for public events, even inside, to block facial recognition software. Nearly a decade later the company was almost unrecognizable. Executives had morphed the

firm into a suit-wearing US government and military contractor that was later acquired by Amazon Web Services.

Wickr's smartphone apps allowed encrypted text messages, photos, and phone calls. Messages deleted themselves after a certain amount of time, which made them unavailable to those who may steal, or seize, the device. The company had a free version of the app that anyone could download, but the money came from Wickr's contracts with private businesses and especially the US government. The "Enterprise" version of the app could be configured to silently send a copy of every message to a central server. Here, government or corporate workers could review copies of messages and documents if the need ever came up. Wickr's encryption worked until the day its clients needed to take a peek at what their workers had been typing.

The Anom app wasn't on the Google Play Store, like an ordinary Android app may be. This was strange to Athit, but superiors told him that the eponymous Anom company loaded the app onto phones itself and then sold those phones to corporations that wanted to keep their internal communications secure. Because of that client base, Anom also required a message archiving solution. Anom, inspired by Wickr's approach, took it and ran with it.

When Athit first joined Anom shortly after his interview, the company immediately threw him into the deep end. Anom's team of then a handful of people was in a coding sprint to finish a proof of concept of the app, including the archiving feature. Anom's CEO Afgoo, an enigmatic figure whom Athit very rarely spoke to and never met in person, had demands from clients to deliver the app on a tight deadline. Bugs needed fixing. Features had to work properly. And it had to be done now.

From his bed Athit got to work. Building an app that deals with sensitive communications is not straightforward, and it has to work nearly flawlessly if customers are going to rely on and pay for it. The team faced an extreme amount of pressure to create a stable version of the Anom app. For the amount of work in front of Athit, the pay was bad: just over $1,000 a month, less than a quarter of what he would later make with other companies.

At the end of the sprint, the code for the Anom app was a cobbled-together mess. Rather than carefully removing sections of code they no

longer needed, the coders just commented out large sections. This was equivalent to scribbling out sentences in a draft of a letter but then putting the entirety of the letter into an envelope and sending it on anyway, scribbles and all. Large chunks of the code were copied from an already existing messaging app available online. The time pressure showed itself in the hastily written lines of code.

But it was done and ready to be tested. Athit and the other developers had no idea they had been hired, in effect, to build a surveillance apparatus.

As Athit lay on his bed with his MacBook on his chest, someone else thousands of miles away to the south was in a nearly identical position. This person held a laptop on their stomach as they sprawled out, barefoot, on a sofa at home in Canberra, Australia. Athit didn't know this man, but he was also involved in the development of Anom. He was checking if the message-copying feature worked correctly.

The man filmed his test so he could later show it to his colleagues. As the man wriggled around with a TV playing in the background, he rested two phones upright against his laptop, one on each side of the screen. In essence, the demo was a mini version of what Anom was supposed to do, with the laptop acting as a stand-in for the server that would archive messages that users sent with the app.

As the camera continued to roll, the man typed the phrase "Ill chase next week" into one of the phones as an example message and pressed the send button. Near instantly, the message arrived on the second phone and also appeared on the laptop. The message-copying system worked, and in near real-time too.

The backdoor was a success. The person lying on the sofa testing the message-copying feature was the AFP tech liaison CIN325, from the agency's Digital Surveillance Collection (DSC) unit. The plan was for Anom to send a copy of every message its users wrote to a server controlled by law enforcement.

CIN325 gained another nickname after his barefoot demo video —"Toes." He acted as the bridge between the AFP's DSC and the FBI. CIN325 funneled questions and updates between the two agencies and Afgoo and chatted with him almost every day between June and September 2018.

These messages flickering on the laptop were the confirmation the FBI and AFP were after. Afgoo had delivered.

Work inside Anom stabilized after that initial rush of coding. Every weekday morning Athit logged in to the team's group chat if he wasn't already. There Athit saw what had to be done, along with the four or five other Android developers who eventually worked on Anom. For seven to eight hours he fixed bugs reported by Anom's customers, such as messages that failed to deliver or images that corrupted when sent—crucial things to sort out for a private messaging app. Athit gained a reputation among his colleagues for fixing some of the most critical bugs in the app. More developers handled Anom's backend infrastructure, and a dedicated team tested the app before Anom pushed updates out to customers. The startup used software to track its coders; it kept a tab on when and how much they worked and sent screenshots to the company. As long as Athit clocked in for his contracted hours every week, he was good. The software wouldn't be able to tell if he was in bed or not.

Like Athit, much of the rest of the team worked remotely, spread around Asia. Around a half dozen members lived in Bangalore and discussed plans to code out of a coworking space in the city. A few junior members who lived elsewhere in India even moved from another state to Bangalore to work on the project. One team member previously worked for the contracting giant Accenture, which provided content moderation services for Facebook. Another worked for the phone company Ericsson. Several others came from a TV streaming company to develop Anom.

Working at Anom was, for better and for worse, just like any other small-time app development company, with group chat jokes and digital water cooler banter. There was an air of secrecy around certain things though. Anom kept its app developers siloed from the rest of the company, especially the resellers who Athit believed sold the app to businesses. Athit's main point of contact was the project manager, who most of the time relayed information to Afgoo. There was no transparency, Athit thought.

Once the phones were loaded with Anom's software, someone needed to get them on the street and in front of customers. Someone with a network of customers looking for a new encrypted phone in the vacuum left by Phantom Secure. Afgoo found a hungry and willing accomplice.

Footnote

1 Author has changed this person's name.

Chapter 11

Roll Out

Domenico Catanzariti was supposed to go into the family business of olive oil. In one photo used to market his family's company Olives 2000, the Italian-Australian presented a lovable image with a head of tight dark curls and a goofy smile. He wore a long-sleeved shirt over a button-down with his nickname and the company's logo embroidered on the front, and gleefully cupped a mix of black and green olives in his hands. "The greener the olives, the stronger the olive oil," he said in one of many bits of olive-related advice in a media interview promoting the business. "A milder (oil) is not so strong, so the olives were half ripened, half green; it's a softer oil but still good flavors."

But Catanzariti didn't stay with olives; he pivoted instead to methamphetamine. By the time he was recording the olive marketing videos, Catanzariti had already dabbled in the drug trade. In 2012 after intercepting a series of phone calls, Australian police raided a methamphetamine lab that Catanzariti was connected to. The lab was in Bibaringa, in a shed of a family home on a working vineyard. It wasn't clear how much of a role Catanzariti played in the drug operation; he at least knew the individual who delivered a trailer to the lab where he understood drugs would be cooked. The police also arrested two other men, and Catanzariti pleaded guilty to manufacturing a large commercial quantity of a controlled drug. The judge gave Catanzariti a twenty-month suspended jail sentence in part for his lack of a criminal record, and because of his day job as the marketing manager for the olive business.

“My conclusion that you are unlikely to reoffend is based on your family’s support and that they will never let you do anything like that again,” the judge said during Catanzariti’s sentencing.

He was wrong. Catanzariti’s crimes only grew in scope. He eventually trafficked larger quantities of drugs including cocaine. Catanzariti also sold Phantom Secure phones, so often that his mug shot appeared in a list of encrypted phone sellers compiled by Australian authorities. In that photo, he already looked much different from his earlier, happy-go-lucky photo shoot for the olive business. Here he looked haggard, with large dark circles underneath his eyes. The long-sleeved shirt was replaced by a blue hoodie. His tight curls had grown into a mess.

Catanzariti found himself without a product to push when the FBI shut down Phantom Secure in 2018. Maybe he could go back to selling olive oil full time, but then Afgoo reached out with a tantalizing alternative: I am making a new encrypted phone, and I need people to sell it.

Catanzariti jumped at the chance to join Anom. Here was a fresh company, with a new, exciting product, that with Phantom Secure now dead could fill a massive gap in the market. He knew the CEO personally from earlier work in the encrypted phone industry. And Catanzariti saw a payday: The returns from getting in early with a new company before it took off could be fantastic for his wallet. He could be closer to the top of the pyramid scheme and eventually manage people underneath him.

Anom sweetened the deal by simply giving Catanzariti the phones for free. Seeding Anom in the criminal community was more important than immediate sales; if Anom blew up, it would pay off dividends later, for everybody.

Catanzariti became Anom’s first on-the-ground seller and settled into his new job. His colleagues from Anom headquarters found he was emotional and often funny; he would moan about some issue and then go back to normal the next day like nothing had happened. His nickname was Messi, an apparent reference to the Argentine soccer star Lionel Messi.

Catanzariti was not selling the Anom phones to corporations, as developers like Athit expected. Catanzariti, obviously, sold them to criminals. Catanzariti harbored connections with Italian organized crime, especially those in Australia who had long benefited from the country’s

drug trafficking. Police suspected he was a senior member of the ‘Ndrangheta, otherwise known as the Calabrian Mafia.

At first, Anom provided just five phones to gauge interest and see if anyone wanted its product. Anom’s phones were a major upgrade over the aging Phantom Secure BlackBerries they may have been used to. Anom used Google Pixel and similar Android devices as its hardware base. The encrypted messages themselves were closer in appearance and feel to something like WhatsApp or Facebook Messenger—instantaneous, real-time—and not the sluggish emailing back and forth that Phantom Secure was. Users could send photos and videos taken with the onboard camera. Earlier companies had removed the camera hardware entirely for security reasons. Since then, encrypted phone firms realized there was a limit to how many features they could remove before clients started asking for them to be put back in. This was the late 2010s—everyone needed a camera on their phone to snap pictures of their product.

Anom’s additional features read like a shopping list for the security conscious. Messages automatically vanished from a user’s device after a certain amount of time, from thirty seconds up to seven days. The servers were said to be hosted outside of countries belonging to the Five Eyes alliance of the United States, United Kingdom, Australia, New Zealand, and Canada, as well as the European Union. A secure vault on the phone could be used to store sensitive files, locked away from anyone who might get their hands on the device. Users could, of course, ask Anom to remotely wipe their phone if the cops managed to get hold of it.

The software also had a novel way of protecting itself from prying eyes. To read their messages, an Anom user first needed to open up a calculator app on the phone. This calculator looked innocuous enough and worked as expected. But once the user entered a PIN and then held and pressed the equals sign, the phone peeled away the calculator facade and revealed the real Anom app underneath. The calculator was, in fact, a password entry screen hidden in plain sight. If a user typed another code, known as a duress password, the phone would wipe itself, permanently destroying all data stored on it.

As for the future, Anom already had an ambitious road map for upcoming planned features that would help it rise above the competition. Those included push-to-talk-style voice messages and a scrambler that

would slightly distort the voices in those recordings, leaving the messages intelligible but the sender's identity obscure.

When turning on the phone, customers would be able to load the device into a special mode where the screen displayed a bunch of innocuous-looking app icons. Instead of the Anom app, the phone would only show things like Candy Crush, Netflix, and Tinder. The apps didn't actually work properly, but the idea was to trick a border guard or someone else inspecting the phone so they would not find the Anom app itself with a user's sensitive communications.

The actual security benefit of these features was debatable—surely police would eventually catch on and know to look for the calculator login screen or the fake Netflix app—but a bit of security theater might pull excited customers in.

But one Anom feature promised to be a true and important security tool. Anom planned to introduce an entire operating system for its phones geared around privacy and security called ArcaneOS.

ArcaneOS would make substantial changes to the underlying software that powered its phones. Those included removing as much Google code from its phones as possible. On normal Android phones, Google aggressively tracked its users, and sometimes made that collected data available to law enforcement. ArcaneOS would do away with that.

Anom said ArcaneOS would not have the ability to make emergency calls to police, fire, or ambulance services, in case those systems could in turn be used to track the phones. The code that controlled GPS was removed entirely, making such tracking impossible, Anom promised.

The custom OS would also make the phones more difficult to hack. ArcaneOS would use a hardened "kernel," the heart of the operating system that, if a hacker broke into it, provided access to the whole device. By reinforcing that kernel, ArcaneOS turned a squishy weak point into a digital fortress.

This was a ton of work for Anom's coders. So the plan was to build ArcaneOS off an already developed security-focused operating system. That template was GrapheneOS, developed by Daniel Micay. Micay, who had a habit of sending a string of a dozen messages at a time when he spoke in online chats, slaved away at GrapheneOS and released it for free for anyone to download and use. He was the antithesis of the underground

encrypted phone industry. While companies like Phantom Secure sold their technology for profit, Micay tried to get secure technology into as many people's hands as possible.

Even Snowden recommended GrapheneOS to the privacy conscious. "If I were configuring a smartphone today, I'd use Daniel Micay's GrapheneOS as the base operating system," he tweeted. Anom did just that. The company took GrapheneOS and used it to build the foundation of ArcaneOS as part of its for-profit underground phone business.

"If you really want to be secure there is only one word: ANØM," a marketing pitch sent to potential customers read. The marketing left out one key detail—who was really running the company.

When a small team of three AFP officers walked into a windowless room in their Canberra headquarters in late 2018, a whiteboard greeted them with a message that one of the officers had scribbled: "The obstacle is the way."

The full quote this shorthand derived from has long been attributed to Roman emperor and Stoic philosopher Marcus Aurelius: "The impediment to action advances action. What stands in the way becomes the way." In other words, only when an obstacle seems insurmountable can you find the motivation and creativity to overcome it. For the AFP around two thousand years after Aurelius potentially penned those words, the obstacle was the encryption used by drug traffickers. And now that same encryption seemed a perfect way to catch them.

The windowless room the officers huddled in, given its need to be locked down, was dubbed the Bunker. Armed with not much more than office equipment and computers, the AFP officers prepared to see if Anom had harvested actual criminals' communications.

Sitting at his desk around Halloween 2018 in the Bunker, one of the officers saw a string of intercepted messages come in discussing crime. The officer was immediately excited. For the first time, in what the AFP dubbed Operation Ironside, they saw messages come from inside an encrypted phone company. To Australian law enforcement, this was the Holy Grail.

These texts were sent by Anom users and now, almost like magic, appeared on law enforcement officers' screens.

Anom's clients weren't corporations looking to protect trade secrets, like Athit the developer was told. The customers of Anom weren't even criminals who wanted a new tool to evade law enforcement either, as Catanzariti thought. Anom's ultimate clients, in a way, were the AFP and FBI that wanted to use Anom as a surveillance tool. Anom gave the authorities that God-like power of reading Anom users' encrypted messages without the users even being aware.

The AFP didn't design the Anom backdoor, but it did create the system that stored its messages for the authorities. CIN325 provided the original collection servers that stored Anom's communications. The DSC then built infrastructure that would allow them to more easily collect and search through the texts. Just like the Anom developers spread around Asia, the AFP encountered its own bugs and errors with the shadow system it built, such as not all of the messages being recorded properly. Both sets of developers worked on the startup, mostly unaware of the others' presence, as if a pane of clouded glass sat between them. The DSC continued to periodically test that Anom worked as it wanted, pinging messages back and forth between Anom phones and watching the texts pop up on their screens. To keep the audacious plan from leaking, members of the DSC didn't say the word "Anom" out loud, even among themselves. In their meetings, they gave the messaging platform a code name that alluded to the specter quietly following criminals: "SmallGhost."

The criminals' own trust in underground encrypted phone providers could be their downfall. The weapon drug traffickers had used for years was now flipped against them. The obstacle was the way. Or rather, it could be, if more criminals actually bought the Anom phones.

The FBI needed a factory. They found it in Hong Kong.

There were no visible signs that the light brown stack of offices on a long, straight road in the city was linked to Anom. One of those offices

belonged to a wholesale electronics company. The glass front doors that opened from the busy street didn't show the name of the company, or that of Anom. The building's windows, littered with rickety air conditioners, blended in with every other high-rise in the city. The eleven-floor tower was one that people strode past every day but may be hard pressed to recall if asked to, sandwiched between more noticeable landmarks like a real estate office and a coffee shop.

Hong Kong was where Anom's code transformed from a scroll of code on a screen into a reality customers could hold in their hands. Anom enlisted the help of this electronics company to install the app onto phones in bulk. The company usually handled the import and export of phones and other goods. The drab office building was one of that company's addresses.

Being in Hong Kong meant the company had little issue getting hold of cheap or refurbished mobile phones to then install Anom onto. This company became Anom's manufacturer and a crucial part of its supply chain.

After Catanzariti seeded Anom with just his five devices, Australia received around fifty more. Anom shipped those to Catanzariti and two other distributors in the country.

With more phones spread across the country, the AFP found a clear indicator the plan was working: the AFP told the FBI that 100 percent of the Anom customers in the beta test used the phones to conduct crimes. Anom's members used the phones to discuss weapons purchases, transporting hundreds of kilograms of drugs, and other illegal acts. What's more, Anom gave the AFP a window into two of the most sophisticated criminal networks in the country. Through Catanzariti, the AFP was tapping Italian organized crime that operated in Australia. The Comancheros biker gang was using the phones too. The gang allegedly even had at least one general group chat in the app for members. Another group chat called "Get It Done" included senior Comanchero members who prosecutors claim discussed luring a target away from CCTV so he could be beaten up.

"Make sure that a proper statement is sent, make sure s**t is broken good," one of the messages allegedly read. Australia was Anom's beta test for the phones themselves and whether the surveillance would work at any sort of scale. Both were on track.

By summer 2019, around eight months after the first Anom message flashed across the AFP's screens in the Bunker, demand for the phones in Australia ramped up. Criminals recommended Anom to one another through word of mouth. Runners drove around Australia to deliver the phones. Anom finally found a foothold in the encrypted phone market. The company could have fizzled out at the start, killed off by a competitor or a lack of customer interest. But here it was, growing into a recognized player in the space.

By that fall, Anom had several hundred users. The majority of those phones were in Australia, but some had spread into neighboring New Zealand. One alleged criminal used Anom to coordinate the transporting of $420,000 worth of gold bullion bars from New Zealand to Turkey.

As popular as encrypted phones were in Australia, the industry was a global one. A next natural stepping stone would be Europe, where the cocaine trade was rapidly expanding. Anom's puppet masters at the FBI wanted to sweep up many more people.

Afgoo started to receive inquiries from customers about shipping Anom phones overseas. Given the globalized nature of organized crime, traffickers in Australia often had accomplices, or masterminds, in other parts of the world. Could Afgoo sell phones to them too?

Chapter 12

Hoops

This was Young's make-or-break moment. Nearly a dozen of his supervisors sat around a conference table on the sixth floor of the US Attorney's Office in San Diego. It was early days, the Australian beta test was successful, but the FBI was not yet reading messages itself. This meeting was for the top official in the office to finally decide on whether the Americans would get to do so.

Young presented to the group what the idea of the FBI secretly running its own encrypted phone company and harvesting those texts might look like. One by one, the prosecutors gave their answer on the idea of Anom: No. Middle management was not impressed. It was a terrible idea. You can't do this, said the seasoned drug prosecutors.

But Young wasn't a drug prosecutor. He didn't carry the institutional baggage of someone who had investigated the issue in the same way, year in, year out. The Department of Justice could be effective at many things, but new thinking was not among them. Maybe some of the culture of a tech startup—disruptive innovation—was what drug investigations needed.

Cheviron's management team at the San Diego FBI were on board straightaway. They didn't need convincing at the prospect of covertly managing an encrypted phone company and tapping its users.

Getting the lawyers around the conference table at the US Attorney's Office to give the green light was another story.

One repeated comparison from those who pushed back was the Fast and Furious operation. In that case, which was still very much in everyone's recent memory, US authorities deliberately let buyers source weapons

through straw purchases, with the hope of tracking the guns to large Mexican trafficking groups. The plan backfired, and the weapons ended up at the murder scene of a US Customs and Border Protection agent. That potentially avoidable death led to congressional inquiries, the Attorney General being subpoenaed, and relentless negative headlines.

There were direct parallels between Fast and Furious and San Diego's Anom idea. The plan was to sell criminals a tool. Even if Anom would be pushing code and not bullets, the phones would potentially still help murderers coordinate. What if a murder for hire were picked up in Anom messages, and the investigators were unable to scramble a team quickly enough to stop that murder, wherever in the world it might be? Would that look like another Fast and Furious–like mistake? What if they missed the crucial message and someone died? The Department of Justice wanted no part in another high-profile disaster.

In response, the team stressed it would be informed about and act upon any threats to life just as it would with an ordinary wiretap. More generally, the Anom team's rebuttal to the Fast and Furious comparison was that if criminals weren't using the FBI's phone, they would end up on any of the other encrypted platforms criminals loved—Sky, Encrochat, Ciphr. The US did not have a backdoor into those. Wasn't it better to at least get some criminals onto a phone that the FBI did have visibility into? Anom would be about intercepting conversations that would be happening regardless.

Young was essentially packing up his things in the San Diego conference room after the echo of nos when the most senior person at the table started to speak. US Attorney Bob Brewer acknowledged the other people's concerns and that it was a risky case. It was really dangerous, and everyone around this table made great points. But, even with that, Brewer said he wanted to see the look on the other prosecutors' faces when they realized we're behind the whole thing.

"This is my decision, and we're going forward," Brewer said. Anom was a great idea. He approved it. The initial barrier of middle management in San Diego had been breached despite a rolling of eyes and shrugging of shoulders around the table.

"We talked at length about the potential downsides, and the upsides were too great," Brewer later recalled. While others in the room may have been concerned with preserving their status as career government prosecutors,

Brewer had no such fear—as a Trump political appointee his term was fixed. Similar to Young, Brewer was somewhat new to this world. Coming from a law firm that focused on white-collar defense and civil litigation, he was the first outsider to get the most senior job in twenty-six years. He wasn't bogged down with how investigations were normally run. As he was in his seventies, this would be Brewer's last job too. He wasn't vying for another, better office someday and could focus on what he thought was doing the right thing, not what was better for his career.

If Anom went wrong, Brewer said he was prepared to go in front of the Senate. But right now he thought it was worth pursuing.

"I never lost any sleep over this," Brewer said.

That meeting was one of the first of many, many bureaucratic steps before the FBI could finally read the messages itself. Young and Cheviron took multiple trips to Washington, DC, where more superiors and agencies chimed in. Some found complicated technical and legal issues. What happens if, say, an Anom user is in Tijuana, Mexico, but their phone technically connects to a phone tower in the United States? That would mean the phone is using US infrastructure and might require more paperwork and authorization.

Other criticisms were, in Young's eyes, less legitimate. Each time superiors brought up an issue, the San Diego team had a solution.

"I think they just thought eventually we'd go away, and we just never did," Young said.

Those roadblocks came to a head when superiors in DC wanted to block Young from the next level of approval meeting. The superiors wanted the FBI agents to go but kept Young off the invite list. Brewer was not happy. He told Young to get on a plane to DC and sit in the hallway until they let him inside the meeting. Young got back in the loop.

At that moment, there was very little appetite from the layers of officials to allow the monitoring of Anom phones inside the US. The rest of the world, where Anom was already starting to expand, was a different story. For now, the team focused on that.

Running the collection of Anom messages from a server in the US might create legal headaches. So the team settled on finding another country that could legally collect the messages on the FBI's behalf, and then digitally

send their contents. To find that country, Young entered yet more meetings, this time in Europe.

The US had opened a case on Sky after they shuttered Phantom Secure. An eventual phase of the FBI's targeting of the encrypted phone industry, Young and the others planned, was to shut down that company too and absorb its users into Anom. But police in Europe had a plan of their own: they were looking to hack into some of the remaining phone companies on the market, such as Encrochat and Sky. At his meetings, Young learned that European authorities were really afraid that Young and his colleagues might indict the owner of Sky before law enforcement managed to investigate and hopefully hack the company. Young assured them: We're not ready to charge, just yet. And even if we were, we don't want to step on your toes. We won't indict until you get a full chance to break into Encrochat's and Sky's bank vaults of messages.

The contours of a grander master plan came into view. One that was even bigger than the FBI running its own encrypted phone company. One that would be more consequential than arresting the CEOs of other encrypted phone companies. The Europeans claimed they could hack Encrochat and Sky—which had something like sixty thousand and seventy thousand active users, respectively.

For the moment the Americans kept their cards close to their chest with Anom. But eventually, combining the intelligence from all three companies would grant law enforcement access to a majority of the underground encrypted phone industry. The only other major phones on the market were Ciphr, which was popular in Australia, and another called No.1 BC. Between Anom and the hacks, government authorities would be able to see more than half the encrypted phone messages being sent around the world. The messages of over one hundred thousand Owen Hansons and their minions could appear in front of the agencies' eyes. The master plan was less a takeover of any one company than a complete undermining of the industry at large.

There was no guarantee such a plan would work. The European authorities still needed to hack into each provider and obtain user messages. Failing that, the US could still charge Sky's owner, assuming there was enough evidence he was committing a crime. Young was skeptical. He thought, "This is never gonna work."

The US team still had a more pressing matter to sort out first. The FBI needed legal access to the messages. Australia, despite successfully running the beta test, was not legally allowed to share the contents of Anom communications it had collected with a foreign agency.

Discreetly behind the scenes of the European meetings, Young and the team started to let other individuals and countries know what the Americans and Australians were up to with Anom. The team set about finding a European partner for the Anom operation. The US needed another country to legally collect the Anom messages on its behalf, and then provide them to the FBI. “Can you do this under your laws? Can you basically help us monitor these phones in some way?” Young recalls asking potential candidates.

In the summer of 2019, negotiations started with one member of the European Union to fulfill that role: Lithuania. Those discussions continued throughout the fall, and the country agreed to obtain a court order to collect the Anom messages. One absolutely essential part of that relationship was confidentiality. Lithuanian officials never publicly said why, but they did not want to be named as the country that wiretapped the world for the FBI. So Lithuania became what US officials discreetly referred to as the “third country,” after the US and Australia.

To avoid the tricky issue of monitoring phones in the US, the FBI designed the system to block out messages from any phones that happened to land within its borders. The Australian authorities, not hampered by US privacy laws, would monitor those phones for threats to life on the FBI’s behalf but not share the contents of the messages for legal reasons. The building blocks of the operation were coming together. All that was left was to get final approval from DC. And with the Department of Justice being skeptical, that took time.

“That middle management sector in DC across those organizations were just enormous obstacles that we had to get through. And a lot of the hurdles that they threw up were man-made, in the sense that I don’t think they were actually principled positions. They were just trying to stop us,” Young later

recalled. “My mantra the whole time was, fly low and fly fast. We just need to stay under everybody’s radar as long as we possibly can and get to the point where they can’t screw us, more than they’re going to screw us, because we’re so far along,” Young said.

Young thought some members of the Department of Justice wanted to kill the operation. If this blew up in their faces, people could lose their jobs, their corner offices, their careers. “They took ten years to get that window, they’re not gonna let some cowboy in San Diego ruin it for them,” he said.

That perception of being the outsiders may have eventually paid off. In yet more meetings in DC, the underlying sentiment was that there was no way the team was going to pull this off anyway. The case didn’t look appetizing enough for anyone in DC to steal it from the San Diego prosecutors and run it themselves. Really, what were a bunch of prosecutors from the border town going to do? If the case actually had a chance of being successful, superiors would have yanked it from the San Diego team’s hands and given it to a much more prestigious district. The Southern District of New York maybe, Young thought.

Those low expectations were ultimately a benefit for the prosecutors and FBI. Go nuts, the DC lawyers said.

Later, Cheviron called Young with the news: we just got approval, we’re good to go. For Young the moment was anticlimactic. Rather than a moment for celebration, it was, finally, time to start the actual work of digging through Anom’s messages.

The FBI created a name for this bold new operation: Trojan Shield. The very thing that organized criminals used to defend themselves would be turned into a weapon to take them down.

More importantly, the FBI took the tiny startup under its wing and started to provide the necessary financial backing to ramp Anom up. In Silicon Valley, venture capitalists poured their money into what they thought might be a hot new company. The hope was for the company to become a hit, and for the investors to cash out their winnings later. The investors sometimes provided business advice and acted as mentors for the typically young founders, which stirred the startup’s direction from behind the scenes. Often the public never knew about these backroom North Stars who stealthily guided decisions for companies.

With Anom, the FBI was to do the same thing. It became an investor in the criminal underworld's latest startup. Only here, the return was not primarily financial. It was instead to build an unprecedented surveillance platform. The FBI would not necessarily manage the day-to-day running of Anom; that was left up to Afgoo and his employees. But the FBI was to become a constant, shadowy presence in the background of Anom, pulling levers and making decisions while Anom's workers and users were completely oblivious to their involvement.

With the third country now secured, the FBI flipped the switch. The agents' screens flickered to life.

Chapter 13

Batman

On his first day inside the San Diego FBI office reviewing Anom messages, newly minted Special Agent Marshall Muse was trying to figure out what "Batman" meant. Displayed on an FBI screen with a black background and lime green and bright white text, a collection of Anom chats kept mentioning the superhero: Prices for Batman. Distribution for Batman. Transportation for Batman. It was unlikely the Anom chats, arranged in a grid with columns for the time sent, the sender ID, and the content of the text messages, were referring to the customers' favorite comic book character.

"I'm a new guy, and I'm like, okay, Batman is probably code for something. I don't know what it is yet," Muse later recalled.

Nestled in their nondescript cubicles and snacking on stale Twizzlers, eventually thirty to forty FBI agents like Muse read the Anom messages. Every Monday, Wednesday, and Friday like clockwork, Lithuania delivered a fresh batch of messages to the FBI. The agents then pored over them, panning for gold in a constantly flowing stream of intelligence. Usually with a wiretap, most of the conversations are not relevant to the investigation. Agents then picked out only the pertinent chunks. With Anom, the FBI agents saw the opposite. To them, the conversations on Anom were overwhelmingly criminal in nature.

The central hub of the San Diego FBI's 253,000-square-foot campus where this took place sat directly in the flight paths of planes landing at the city's nearby airport. When agents were speaking outside, the roar of the jet engines would sometimes completely drown out their conversations. The

building looked more like a tech company's headquarters than a law enforcement agency outpost. The vestibule entrance was a cube with three of its faces made from glass, letting in a flood of light not unlike an Apple Store. HGA, the architecture firm that designed the San Diego field office, also worked on Dropbox's hip headquarters in San Francisco. Fitting, given that this FBI campus was where the agency secretly ran its own startup.

Other elements reminded visitors that this was still an FBI facility. The parking garage was coated with a mesh-like fabric that helped preserve the anonymity of those working in the office. Just over a dozen palm trees ran parallel along the facade's tall glass side, and three flags were planted at the base of the entrance steps: the United States flag, California's flag, and one with the FBI emblem. The reception area housed angular coffee tables and Art Deco black leather seats. An approximately ten-foot-wide FBI seal hung on the wall. Inside the building proper, mug shots of the FBI's Most Wanted criminals and abstract art clung onto long, white corridors. Agents worked out in multiple well-stocked gyms.

Deep inside this fortress on the second floor was room 2415, called the "technical center," where agents read Anom's messages. At the head of the operation were Cheviron and Stevens, the two agents who would oversee the gargantuan task of running a secret FBI startup. Those de facto co-CEOs read the messages too, but this was no longer an operation involving a couple of prosecutors and a handful of FBI agents. In January 2020, the team pulled in the rest of the Organized Crime Squad, a team of eleven agents that included Muse. FBI computer scientists created an in-house system called Hola iBot for displaying the messages on agents' screens.

Muse was still learning how that system for reading the Anom messages worked when he was greeted with the Batman puzzle. Later during that first day on the operation, he got his answer. One of the Anom users sent a photo across the app. Muse pulled it up on his screen. He didn't know how many kilos it was, but it was now clear what Batman referred to: cocaine. This drug syndicate had brandished the Batman logo on blocks of their product and given the cocaine the group's own calling card.

A familiar person was behind some of those Batman messages. It was Catanzariti, the distributor who had first seeded Anom in Australia. He had climbed the criminal ladder since his days of helping with the setup of a shoddy methamphetamine lab in the Australian countryside and was now a

high-ranking drug trafficker. In December 2019, Catanzariti said that an associate called Salvatore Lupoi sent him a photo. It showed hundreds of kilograms of coke stamped with the Batman logo. The tightly wrapped packages sat in tall stacks next to one another, with what appeared to be a label gun nearby. The following month, the pair picked up the conversation about Batman again.

Catanzariti wasn't the ultimate supplier of the cocaine. That title went to someone he referred to in the chats as Atlas. The photo, Catanzariti wrote, "was all atlas stock," and he wondered whether Atlas had "got it in." Catanzariti and his associate then discussed the pricing for each kilo of drugs. The pair agreed that $160,000 AUD, or around $100,000, was the maximum price.

Neither man had any idea that on the other side of the planet, Marshall Muse was watching the Batman trafficking plans play out.

After Muse's first day solving the Batman puzzle, he spied on other Anom users who were, to him, much more frustrating. One target he zeroed in on had acquired a bunch of Anom phones but hadn't committed any crimes with them. Instead, the man used the phones to speak to his various mistresses on the down low. Muse said the messages he saw pop up on his screen were what you might see in typical boyfriend and girlfriend conversations. Dick pics often flowed across Anom. Sometimes criminals didn't only send these pictures to their romantic partners but to their business associates too. "Got another one" the agents joked when the images flashed on their screens.

With the girlfriends Muse was monitoring, no crime was yet underway. But Muse kept reading. In the San Diego FBI's eyes these girlfriends, and others who weren't yet committing crimes, were still valid targets. To the agents, if you were on Anom, you were a target by definition because the FBI believed the company was supposed to be only for criminals. Even if you just happened to be dating someone who bought you an Anom phone.

The rationale was that these sorts of people might know about the destination of drug shipments because of whom they associated with.

The legal fact was, the FBI didn't have to only monitor criminals. The data from Lithuania arrived with virtually no strings attached. Legally, the FBI could read any messages that pinged between Anom phones outside the US that they wanted to.

In the rare instances the FBI came across a civilian using Anom, the agents tried not to monitor those phones as intently as others. If an attorney happened to use an Anom phone, the FBI was stricter on whether it could read those messages to keep in line with the sort of monitoring that would, or would not, be allowed under a traditional US wiretap. The agents also had a way to stop sweeping up messages of particular phones if they wanted to.

The FBI decided when to intervene and stop a crime in progress and when to let criminals do their thing. The FBI was happy to allow some crimes to play out—some drug deals here, a shipment there—if it meant collecting intelligence on other ones. They played God in which crimes were allowed to be successful and which were not. Some crimes ultimately weren't worth burning the entirety of Anom over.

There were cases where the FBI had to act. The man who spoke to his girlfriends on Anom had a reputation as a bad boy. That was why Muse kept reading his and his mistresses' messages. "I know this guy, and he's going to get into something," Muse said.

Eventually, one of the girlfriends slipped up. She had fallen out with a friend who worked at a particular hair salon. I hate her now, I need you to do something about it for me, Muse later recalled her writing on Anom. I need you to be a bad boy for me and do something, Muse paraphrased.

The boyfriend decided to firebomb the salon. Muse watched the process unfold in front of his eyes. The target recruited people for the job, and the person who ultimately bombed the salon sent proof of the attack back over Anom. Muse saw the entirety of the violent act, from inception, to planning, to execution.

Beforehand, the FBI provided notice to the relevant authorities. A tip-off might result in an arrest or an attack being thwarted; or the tip could be too late. Ultimately it was up to law enforcement in the respective country to decide how to intervene. In this case, the firebombing still took place.

Other agents who worked on the Anom messages hunted out these sorts of violent acts specifically. One of those was Brett Kalina, who was technically Cheviron and Stevens's superior, but he also got his hands dirty with Anom. Bald with a huge grin, Kalina sometimes friendly-slapped the back of people he was talking with.

Kalina's job from day one of the FBI turning on the switch was to pore through all of the photographs sent across Anom. The first thing he did was look for threats to life—signs that criminals planned to beat up someone or kidnap them. Or, as what became a regular occurrence, plotted to kill other people. In this stream of pictures, Anom users sent photos of the people they wanted to harm, or the weapon they wished to use. A victim tied up in a basement. The planned getaway for assassins. What explosives to purchase. Legally the Anom operation wasn't what the US judicial system would think of as a wiretap. But the FBI treated it ethically as such. The FBI had a responsibility to respond if it thought someone's life was in danger.

Every day, Kalina scanned these pictures. The next steps were identifying who exactly was the intended target and getting that information to a law enforcement agency that could act on it. In texts Anom users explained how exactly they wanted to kill certain people. Other times Anom only provided a piece of the puzzle, but the agents had to make do with what they had.

In those threats to life, ever growing piles of dynamite spread around the world. Explosives the FBI could only look at and not defuse themselves. And every bomb defused carried the risk that criminals would get wise to how police seemed one step ahead of their plans.

"We had to take quick and decisive action to do our best to prevent any loss of life," Kalina said. There was always a rush to finish reading through Monday's messages before another batch on Wednesday, when even more potential threats to life would arrive. "Threats to life were a big, daily chore," he added.

Kalina had rushed to help others before. In June 2016, a man killed forty-nine people in a mass shooting inside Pulse, a gay nightclub in Orlando, Florida. Immediately after, Kalina and a group of other LGBT agents volunteered to travel to Orlando to help out with the response. The group trained therapists and other service providers on the use of pronouns

and other sensitivities and helped set up a family assistance center. Kalina told a news outlet at the time his team worked with one mother who "was way more upset that her son was gay than that he had been shot." In other cases, the assistance was for a victim's chosen family, not their biological one.

Many more FBI agents were tracking their own targets. Each time Young visited the wire room, he noticed more and more organizational charts of names and faces on the wall, schematics of different syndicates the FBI had put together. The first time there were one or two charts. Then when Young visited again, over half a dozen. Then twenty-five. Eventually, he estimated there were sixty. The FBI was doing the same sort of work Young had helped with years earlier, of reading Hanson's messages and mapping his crew. Only now the FBI was doing it for dozens upon dozens, and later hundreds, of distinct criminal organizations—that painstaking investigative work of finding who was who in the messages, but now on an international scale.

Many of these people were a complete mystery to the FBI. In some cases the FBI didn't know anything about them, only where they were located. They mapped out the syndicates regardless.

The agents were able to build maps of these networks because the system at their fingertips did much more than sort the texts into a presentable format. With a click of a button, the system visualized which other Anom users a target spoke to. The agent's current target sat in the center of a spiderweb as a red circle. The agents could drill down into that user for more specific information, such as their phone's unique serial number, what phone network they connected to, and all photos the user sent. This was displayed in a sort of profile of the target, not unlike a Facebook page. The profile also showed what languages the target typed in.

Then around that red circle, blue circles symbolized other users the target spoke to. Finally, lines from those circles led to a larger, green circle. This represented a group chat those contacts shared. The right-hand side of the screen provided summaries of what the messages said, meaning investigators didn't have to read through the actual texts over and over again when following leads.

The agents could then click on any of the other users in front of them, repeat that process, and in turn see whom they spoke to. They then grouped

users who frequently associated with one another into distinct syndicates and named them after gods from Greek mythology such as Zeus and Morpheus.

Mapping out an Anom user's social circle wasn't always straightforward. The FBI agents found that when a new person signed up for Anom, they often communicated with more than one syndicate at a time. Rather than sit in an isolated cluster, users might act as a bridge between several. Some users moved between multiple criminal groups and resisted any analysts' urges to place them into a single syndicate. These inconveniently placed circles highlighted something fundamental about organized crime in the twenty-first century: criminal groups don't act in a vacuum. In a globalized world, organized criminals are more connected to one another than ever, and Anom's interface of linked circles showed that in the clearest possible terms. Those overlapping, changing crime networks spread out day by day and week by week, a vast and expanding universe of drug traffickers.

There was also one other person a new Anom user often spoke to when first getting online: their Anom phone distributor, who likely ran them through any troubleshooting and helped them log in to their Anom account. Once the new user had gotten accustomed to the Anom phone, the communication diminished.

When the San Diego FBI first grabbed Hanson's encrypted phone from him in a car park and whisked it away years earlier, they had to take photos of the messages one by one. Then when Katz and Young rummaged through those photos, they were stuck with painstakingly entering pertinent data into an Excel spreadsheet or other archaic means. With Anom, the FBI had automated the entire process, from collection, to archiving, and to mapping out who was who. They policed at scale.

As the agents silently tracked drug traffickers through their computer screens, they were armed with things other than text messages. From its inception, Anom steadily released new features for its users to enjoy.

Scrambled voice messages. A secure vault for storing sensitive files. A photo editing feature that would pixelate faces before the user sent the image. These helped Anom differentiate itself from rivals on the market. Anom cared about its users' security—what other company was iterating as quickly as Anom?

The developers across Asia worked hard on these features, squashing bugs and making them solid enough to roll out to customers. They didn't decide what features to create or know why some of them had unusual additions. The coders just followed instructions from their immediate superiors, who in turn took orders from Afgoo.

Unbeknownst to the developers, the FBI puppet-mastered what got into the app and what didn't. Every single one of those privacy-enhancing features had a secret. With the voice memos, the authorities could obtain an unscrambled version. The secure vault was more like a paper fort; it automatically uploaded its contents to the authorities. The photo pixelating feature provided a copy of the unaltered image to law enforcement. And the remote wipe and duress password features were ultimately futile; even if a user wiped their phone, Anom had already sent their messages to the authorities. For every feature Anom users thought gave them more security, the FBI had a workaround that actually gave the agency more data. Now all of that harvested data sat in the backend system for Muse and others to dig through.

"There was always some hidden feature within that that benefited law enforcement," Muse said. Muse watched as the Anom users took photos of themselves at nightclubs and at home. They sent selfies, a lot of selfies. They snapped images of their friends too, all the while oblivious that they were making the FBI's job to identify who was using the phones easier. Then the users uploaded details of illicit enterprises into the secure vault. "Oftentimes it would be drug ledgers, price lists, information on businesses, whether they were legitimate or fronts, shell companies, bank accounts. They saved all of this into their vault, assuming that it was safe," Muse later recalled. Anom's apparent commitment to privacy made the company's criminal users trust the phones even more, when those features were in fact its users' death knells.

It didn't take long for the FBI to see messages that applauded Anom's security, with many users saying even the FBI could not penetrate the app.

The agents in San Diego threw a big yelp when one of those texts rolled in. It became a regular occurrence—over and over, criminals praised Anom for being secure, while those same messages then flashed on the FBI analysts' screens.

"It never gets old," Muse said. "It was the best feeling for me as a new special agent to the Organized Crime Squad, to be sitting there, reviewing my messages, and just chuckling to myself, as these guys in whatever foreign country are going back and forth, talking about the FBI."

Even Anom's crown jewel, the ArcaneOS operating system, was a lie. The pitch to customers was that ArcaneOS shut off any GPS features. When a user tapped through to the settings of their phone, the option to turn location tracking off or on wasn't even there. Anom had removed it entirely.

Whereas that might signal to customers that the capability for GPS was gone, the custom operating system in fact did the opposite. ArcaneOS secretly provided the ability to track the physical location of nearly every device and, by extension, the real person who carried the phone in their pocket. Once ArcaneOS enabled that tracking, the Anom app itself then tapped into it and attached the user's precise latitude and longitude coordinates to every message before it sent the text to the authorities. Thanks to ArcaneOS, the phone did all of this without asking, or alerting, the user.

Athit, one of the developers in Asia, was tasked with building this GPS tracking code into the Anom app. He, of course, did not know the demand for such a spying service came from the FBI. As far as he knew, Anom was still serving its corporate clients.

Athit didn't even know all that much about ArcaneOS either. Afgoo siloed the company. He had another team of developers who worked only on ArcaneOS and didn't follow the normal chain of command. The ArcaneOS coders reported directly to him. There was some cross communication between that team and that of the normal app developers, but only to fix occasional bugs.

Whereas the Anom app itself was a mess, team members thought ArcaneOS was a work of art. The operating system provided complete and total control over the phones. On another system separate from the Anom surveillance interface that Muse used, ArcaneOS provided a satellite-like view of the entire phone network. Dubbed "Arcane Manager," that light

blue, black, and white panel showed how many Anom phones were online at any one time. Here, those with access were able to push updates to Anom's phones no matter where in the world they were.

The geekier employees at the FBI and AFP were very excited to have complete control of the operating system. The possibilities for that were endless. ArcaneOS transformed the Anom phones from eavesdropping devices into cogs of a powerful surveillance machine.

"I'd just be shaking my head, thinking, this is, number one: really cool. And number two: this is the kind of work that we should be doing," Muse said.

Chapter 14

Kings Cross

The cafe of the Kings Cross hotel was a hidden gem in Istanbul, Turkey. Stylish lights hung from the ceiling, and comfortable chairs were dotted around. A full espresso bar pumped visitors with caffeine. A glass cabinet housed an eclectic mix of cakes and treats. On a high shelf behind the cafe counter, a ceramic blue eye—a traditional symbol for warding off evil spirits and absorbing negativity—watched over those in the room.

In the cafe in March 2020, four members of Anom plotted how to expand internationally. Dialing into a laptop over Zoom was Afgoo. In the cafe itself was reseller Aurangzeb "Bobby" Ayub, whom Anom had tapped to be one of the company's boots on the ground in Europe and farther afield. He loved the hotel's coffee. Also in the meeting was a Dutch phone seller known as Dragonfly, who had told Bobby about Anom after meeting him in Dubai. Dragonfly had contacted Anom through its website, which could only be properly accessed after receiving a code from an existing reseller. Last of all was the artisanal drug trafficker who first introduced encrypted phones to Australia several years earlier and the owner of the hotel: Hakan Ayik.

Ayik would be the one to rocket-jump Anom's presence throughout Europe. When customers asked Afgoo if Anom could ship phones overseas, Ayik was an obvious choice for Anom's next chapter. Afgoo was the tech expert who vetted Phantom Secure for Ayik when he first went on the run. Now the pair were back together with Anom, albeit this time over Zoom, and with Afgoo secretly working for the FBI.

Ayik was still active on social media. He frequently used Twitter to retweet Donald Trump and stories about Turkish President Recep Tayyip Erdoğan. Despite his hand being on the pulse of all things tech, Ayik had never used Zoom before.

"It's crystal clear," Ayik said as the meeting progressed, a tinge of his lingering Australian accent coming through. "Zoom is amazing, isn't it?"

As for how to expand Anom internationally, Bobby spoke up. In his soft-spoken voice, he said the group needed to find two or so large groups of encrypted phone users willing to make the jump to Anom.

"I think the best way to go to market is to quietly and safely find the right couple of big groups, and then once they start to roll it out, then everybody start to talk about it. Then you've already got a foot in the door, and you're already there with a couple of big groups," Bobby said in the meeting. "South America, Dubai, and Asia, these are the three markets where all the decision-makers sit." Convince those decision-makers, and the sales would follow.

Bobby said his pitch to potential customers would be that, simply, it was time to switch. In his opinion, Encrochat was too hot now. Bobby knew the big guys were always looking for better, safer technology. Anom could be that new option. Bobby said he planned to go to Dubai later in the year, where he could pitch Anom.

"It's the right moment to pitch the right product," Bobby said.

Bobby understood what clients wanted because he had been in the encrypted phone business for years. He sold both Encrochat and Sky phones. To a casual observer, Bobby looked like a normal Dutch businessman. With short dark hair and a graying beard, he often wore generic blue suits with open-collared white shirts. When he attended an entrepreneur award ceremony as a finalist, he shaved the beard and donned a black tux.

Before selling encrypted phones, Bobby says he held a myriad of other sales jobs. He meticulously spelled out his years of business experience on his LinkedIn profile: 2007—a consultant for the oil giant Shell for three years; 2013—sales development for Asia Pacific and Japan with an analytics company called Qlik; 2014—head of worldwide sales for a startup that sold a product called Loop Email, which organized customers' messy inboxes. Bobby even listed his work in two different managerial positions at

McDonald's in and around Amsterdam over twenty years earlier. Overall, he had more than two decades of experience across different industries with what he claimed was a proven track record of getting people to buy whatever product he was selling.

That product was now Anom. Bobby was different from Anom's other phone sellers, who were often involved in drug trafficking themselves. Multiple people inside Anom saw him as one of the good guys: a smart and level-headed tech salesman and certainly not a drug dealer. He was friendly to work with and greeted his colleagues with a distinctive "g'day." In the meeting, Bobby showed off Encrochat's "portal." It was a special website that only Encrochat's resellers could access. Here, they could manage their customers' subscriptions, activate new phones, and perform administrative tasks. If Anom wanted to grow to any sort of serious size, Bobby felt it needed a portal too. At the moment, only Afgoo was able to do those sorts of things. Anom's current approach severely slowed down how quickly customers could get up and running. Having a portal would make Anom much more efficient. The trade-off was sacrificing Afgoo's complete control over technical aspects of the phone setup and giving resellers more agency. In return, Anom would become a company that could expand more quickly. Afgoo took notes for later.

Bobby said it would be a good idea for Anom to be a more public-facing company. Anom could put a free version of the software on app stores with limited features. When a user wanted to upgrade to the full version, they would be put in touch with a reseller.

One reason might be to make Anom less of a target for law enforcement. If members of the public used a free version of the app, surely the FBI couldn't then shut it down? It was one thing for the authorities to target a platform used almost exclusively by criminals. It was another to shut down something closer to WhatsApp. The police would have a harder time getting away with it.

Ayik paid attention to Bobby's advice. Often people at the top of the industry didn't take interest in what sellers had to say. They just wanted to extract whatever benefit they needed quickly and then move on. Ayik was different. He was interested in what people below him thought. He made time for them and actually listened.

In this case, Ayik wanted to keep Anom underground. That's what he had done for Phantom and Sky. "You know me, I'm always going for underground, and I've always claimed underground is the best way to go," he told the group.

Regardless of the approach, Dragonfly, the other phone seller, had a warning for the group. The competition wouldn't simply step aside. Anom would need to brace for blowback. Encrochat and its main competitor Sky would not appreciate a new player in the industry pinching customers. Dragonfly, in his rapid-fire Dutch accent, made this clear to the rest of the group.

"You can expect when the Encro and Sky people know we are coming to the market, they are lots of people, they are going to attack us," he said. In his eyes, Encrochat played dirty. "Because that's what they do." He was 100 percent sure.

"It sounds like you've attacked people before," Ayik said. The group laughed. Dragonfly didn't deny it.

The next item on the agenda was whether the team would roll out to new markets with Anom's custom operating system ArcaneOS or just phones loaded with the app. Doing the former would require sourcing specific hardware that could run the OS. It would also mean shipping equipment to sellers for installing the software onto the phones. That was too slow for Ayik's taste. He wanted to move fast.

"It goes back to efficiency and getting the product out there. Look at McDonald's, they go and get the burgers out there. You're not waiting. That's why people go there," Ayik said to chuckles from some of the group.

Afgoo deferred to Ayik on these decisions around marketing and sales. Ayik, after all, was the drug trafficking superstar. He was the one who popularized encrypted platforms among certain organized criminals in the first place.

Ayik's stellar reputation among the drug trafficking underworld could be invaluable to Anom. He was what law enforcement came to call an "influencer." Instead of the sort of influencer who convinced their Instagram followers what skin product to buy, Ayik told serious organized criminals what encrypted phone they should use to traffic drugs. The over-the-top and social-media-loving drug kingpin was a perfect face for Anom. More criminals would trust Anom if Ayik got behind it and gave it his

stamp of approval. Without his backing, it would take Anom years to attract the major players to its platform. Ayik could jump-start Anom's popularity and legitimacy.

And for Ayik, Anom obviously presented a shot at another huge payday. Ayik had a chance to score a hat trick of working with successful phone companies. First Phantom Secure. Then Sky. And now Anom across Europe and maybe farther afield as well. He stood to make a fortune. Again.

By now criminals had realized that being involved in the encrypted phone industry was both good for their day job of trafficking drugs and a very profitable investment in its own right. It was a smart move for criminals to diversify their portfolios.

According to the Australian media, Marco Coffen, a former member of the Comanchero biker gang, secured a chunk of encrypted phone firm Ciphr that gave him exclusive distribution rights for the company in Australia. In Scotland, James and Barry Gillespie, who authorities have said are two drug kingpins known as the Brothers and who controlled much of the country's heroin and cocaine importation, went a step further. They created their own encrypted phone company called MPC. Initially MPC was to serve the Brothers' own security needs. Then it sold phones to other crews. That company was literally created by and for organized crime. Scotland Yard believes the pair may have been murdered while in hiding.

Ayik did not need much convincing to become Anom's bridge to the wider international market. Over the past year he had seen Anom grow. He thought it was ready to be rolled out more widely, and it was a mutually beneficial arrangement to him and Anom. Ayik wanted in.

He wasn't satisfied just selling Anom's phones. Ayik wanted more power over the company itself. He introduced himself to at least one person as the CEO of Anom, even though that wasn't true.

One of Ayik's competitors was interested in Anom as well. Not unlike a venture capitalist, they wanted to buy a 50 percent share of the up-and-coming startup. Ayik heard about this attempted takeover of Anom by a rival. Ayik wanted to acquire the company as well.

Ayik knew he wouldn't be able to buy Anom outright. But his lie to the seller that he was the CEO of Anom showed that he wouldn't simply fall into line: he wanted more control of Anom and would do what he needed to get it.

The threat of a rival getting ahead, even if a sale wouldn't materialize, still irked him. Ayik became even more motivated to make Anom succeed.

Another group stood to benefit from Ayik joining Anom. With the AFP quietly monitoring Anom messages in the Bunker, if Ayik joined the company, Anom would silently sweep up his communications too. Inside the AFP, officials had marked Ayik as a priority target. After years of Ayik humiliating the AFP, the agency might be able to digitally peer over his shoulders and track him down. Despite his mocking message on Facebook to the authorities of "catch me if you can" when he went on the run, the Australian police had, in fact, not apprehended him.

Clueless to the trap he was leading himself and others into, Ayik told the group at the meeting, "The whole idea is, we're gonna team up, to work as a family, to be one, to be one team basically, you know."

That drive for collaboration extended to Ayik's drug trafficking empire, which was now bigger than ever. Things had changed in that world. Rivalries became profitable alliances, and there was more cash to be made if Australia's on-the-run kingpins teamed up. They could control the flow, and the price, of drugs as one.

Ayik created what the Australian government dubbed the Aussie Cartel. This group of nine top-tier traffickers was responsible for about a third of all drug importations into the country. The Australian Criminal Intelligence Commission (ACIC), a clearinghouse for information between the country's law enforcement agencies, later said in a statement, "We use the term 'cartel' as they exhibit cartel-like behaviours—they have similar criminal intent, collaborate for mutual benefit, minimise competition between each other and seek to increase profit and influence. They don't call themselves a cartel."

It estimated that the cartel's net profit every year was a billion Australian dollars, or over $600 million. The Australian government claimed at the top of that money printing machine was Ayik. More than a year before the meeting with the encrypted phone sellers and Afgoo in his hotel's cafe, Australian media described Ayik as the country's biggest drug trafficker.

Australian law enforcement claimed all of the men were, like Ayik, originally from Australia but had fled after law enforcement pressure. They were spread across Europe, Asia, and the Middle East. From their overseas bases, the members still profoundly impacted the drug trade inside

Australia. The cartel eventually imported more methamphetamine and cocaine into Australia than any other group. The members being offshore actually increased their threat to Australia, the ACIC believed: their connections to money launderers and suppliers were now even stronger.

The Aussie Cartel demonstrated the increased connectedness between traditionally disparate organized crime syndicates. Some of the cartel members led groups that previously couldn't be in the same room together without violence, let alone work together. Based on reporting in the *Sydney Morning Herald*, in the Aussie Cartel Mark Buddle, the latest head of the Comancheros biker gang, collaborated with his Hells Angels counterpart Angelo Pandeli. Violence still unfolded between bikers on an individual basis, but on a policy level the groups put aside their differences for a common good: money.

The cartel made highly effective use of "doors," access points across a country's borders through which corrupt insiders at government agencies or private companies helped usher drug shipments. While some trafficking groups may have focused solely on elaborate covers to hide drugs, the Aussie Cartel also had people whisk shipments through the front door.

That top-tier status made Ayik the best possible brand ambassador for Anom. By the time of the hotel meeting, Ayik was already using Anom for at least some of his own drug trafficking operations, including one involving hundreds of kilograms of cocaine. In some of those messages he was concise and professional. "Just to be clear I'll point out the jobs that we are already working on and the one I'm mentioning," he sent in one message, followed by a numbered list of narcotics shipments. Ayik was exceptionally polite, according to an associate who worked closely with him. While others threw fits and panicked during high-stress situations, Ayik always kept it cool, they said. In downtime, Ayik would talk with the associate about his kids, taking them to school, and his wife's small business.

That didn't mean Ayik wasn't ruthless. Law enforcement believed Ayik struck fear into the criminal underground with threats of violence. And he allegedly orchestrated robberies of people who once considered him a friend. But oftentimes he ran his operations closer in tone to a legitimate businessman than a street thug.

Halfway through the meeting, the discussion shifted from the expansion plans to what Afgoo was working on with the Anom system itself. The group oohed and aahed as Afgoo ran them through Anom's new features. One was the ability to quickly switch through different eSIMs, meaning Anom phones could work nearly everywhere in the world. Anom could also seamlessly push new regions to the SIM cards, making the user experience even smoother.

"You've got us speechless," Ayik said as others laughed.

Afgoo knew the product he had developed was good. "As far as Anom goes, what you show to the end user, I think will be impressive. It's better than anything out there," he said.

For minutes, and then hours over the meeting, he won the phone sellers over. Afgoo told the truth at the meeting—that their main competitor Sky was based in North America, and that meant it may fall under laws there. He said Apple and Google could backdoor their phones if they wanted to or were forced. "Right now, it hasn't happened, but I wouldn't be surprised if it did happen," he said. Maybe only saying what was true made keeping up the underlying lie easier.

The lie he left out was that his phone was already backdoored by the American authorities. At the same time that he was saying ordinary iPhones and Android devices could be backdoored, he was selling the men on a device that had a direct line to the FBI. Afgoo, of course, did not mention that the phones automatically sent all user messages to the agency.

Ayik was pumped to get moving. He had already shown some people the device and generated interest. "They haven't even seen 5 percent of what it's got, and they just say, get me one, straightaway."

"It is better than anything out there, and it is ready to go," he said.

While Bobby would focus on the Dubai angle, and attempt to give the company some pseudo-legitimacy, Ayik would bring in his own people. Inevitably, those people were drug traffickers.

Just over two weeks after Anom's distributors held their meeting, the FBI agents in San Diego ran into a brick wall. In mid-March 2020 the city, like much of the world, went into COVID-19 lockdown. While everything closed down around them, the FBI found ways to keep Anom's surveillance going. The agents sat in their chairs with an empty cubicle between each to maintain social distancing. The San Diego FBI compared the headquarters

to the empty hotel in *The Shining*, with not many more people than the Anom agents walking its halls. Agents cleared their own desks and left bags of trash outside the door. Left to their own devices, agents rummaged through the building's closets until they eventually found a vacuum cleaner. "Where did you find that?!" others exclaimed.

The FBI also accelerated a plan to make it possible for agents to use the Hola iBot system from home. They already knew they wanted to eventually give access to the data to foreign agencies, but COVID-19 made the need for a remote access tool that much more urgent.

The agents watched through their screens as COVID-19 interrupted the operations of Anom's users too. The FBI saw criminals change in real-time in response to the crisis. Some explored how to smuggle their narcotics inside shipments of masks or hand sanitizer. Money laundering shifted to more use of dead drops, where a criminal leaves cash in a certain place and then an accomplice picks it up later. This meant they never had to be face-to-face, their own way of social distancing.

COVID-19 may have shut down most of the world, but Anom's growth was only just starting. One seller in particular would vow to make Anom the biggest phone company on the planet.

Chapter 15

Microsoft

Sometime after midnight on May 26, 2020, a sleek black-and-white speedboat darted through the sea's waves off the coast of Sweden. The two men on board, armed with navigation equipment, night vision goggles, and fishing rods, had a specific location they were barreling toward somewhere in that deep darkness.

Meanwhile the *Donousa*, a black-and-red 225-meter-long cargo ship, sat motionless in the water around seventeen kilometers away. Originating in Brazil, the ship was en route to Poland but had made this unofficial stop in the North Sea. The ship's crew planned to stay there until three a.m. In that window of time, corrupt sailors threw nets holding four hundred kilograms of cocaine overboard. They had done this sort of gig before. The job of the men on the speedboat was to now go pick up the nets and safely transport the cocaine to shore. The two men had the *Donousa*'s GPS location, and the ship would light up the area "like a disco in the middle of the sea," a member of the drug gang wrote in a text message.

The plan was not unlike the dead drops of the Cold War, with spies leaving notes for each other hidden in walls or park benches. Only this drop was eight packages stuffed with what they believed to be some of the highest quality cocaine produced in Colombia. The men hauled the packages into the boat and sped back to land.

On shore at around five a.m., a courier was preparing to receive the packages and then move them into a white van for stashing in a warehouse. In the early morning, local residents milled around to go to work.

The courier was in an encrypted group chat with three other drug traffickers—two senior traffickers and the ultimate mastermind of the operation. On their Sky phones, the three men sent the courier messages in Swedish. They told him to bring water and Red Bull in preparation for the landing. Remain calm and composed, and check the surrounding area in case people had started to wake up, they told him. Don't arrive too early to the dock where the boat planned to park, and instead do some laps if you need to. But when you do, drive calmly and melt into the rest of the traffic. That was better than hanging around and looking shady.

When the speedboat first arrived, the drivers parked the boat too far away from the van they needed to move the cocaine into. After moving the boat, the men on the ground faced another issue. The packages were so big that they had trouble cramming them in. Eventually, they squeezed in the cargo of bags, and the group was ready to get out of there.

"You'll drive slow as fuck," one of the senior traffickers wrote to the courier. "And won't tell anyone about this!"

About thirty minutes later, the men arrived at a warehouse and started to unpack the massive haul of cocaine. Their superiors wanted them to count package by package exactly how much was in the haul. The disembodied voices on the end of the phone knew exactly how much cocaine there should be. The courier started with photos of the bags on the concrete warehouse floor. Then he sent photos of one of the open bags to show its contents.

By this point, one of the men who had been in the speedboat was exhausted and hungry, having spent all night among the waves without any sleep. He kept nagging about it and got on the courier's nerves. The courier passed his Sky phone to the tired smuggler so the mastermind could talk to him directly and calm him down.

"My brother, are you here?" the mastermind wrote in Croatian, switching from Swedish to a language the man could understand. "Count all the pretty ones together and take pictures. All these people are great and you have nothing to worry about."

The courier counted the cocaine and sent images of the blocks of drugs, now taken out of the bags and laid in rows on the floor. He said there was 305 kg in total.

They were short.

“No, count again,” one of the traffickers ordered. There should have been 400 kg.

“Did you have eyes on it the whole time? How can so much be missing?” another wrote.

The speedboat driver then revealed something that might have been the cause of much of his anxiety: some of the cocaine had been lost in the water when he picked the packages up from the ocean in the first place. The bags carrying them had broken.

The courier was about to freak out, he said. He needed a second to calm down himself, please stop sending messages for a while, he told the traffickers.

After a short breather, the men in the warehouse found another bag they had forgotten about. That brought the total to 330 kg. They were still missing a huge chunk of the shipment. Search everywhere again, one of the traffickers ordered.

“I have checked. He has checked,” the courier wrote back.

He then stacked all of the blocks up against a white painted wall in the warehouse for easier counting and sent a photo of his cocaine structure to his superiors.

“Are you happy?” he texted.

They were not.

“Closer,” one of his bosses demanded. “Get down on your knees,” to take another picture.

The courier sent two more pictures in quick succession, with his phone’s camera right next to some of the blocks. That revealed the emblem stamped onto each package of cocaine: a red swirl. The same logo was embossed on the cocaine itself, a calling card of whoever put the blocks together.

The courier then placed the empty duffel bags next to the columns of cocaine and took a photo of them. He triumphantly stood on top of the bags, pointed his camera down to the floor, and snapped a closeup of his feet, the bags, and the cocaine.

By now it was just before nine a.m. The bizarre photo shoot had gone on for two hours, since the speedboat driver and courier arrived at the warehouse. Other than the cocaine missing in the sea, which one member suggested they rent a helicopter to find, the complicated operation had been a success (members of the public soon found bundles of cocaine washed up

on shore). Losses are a part of any smuggling trip. Later, the group sold the speedboat and the van used to transport the cocaine. They didn't need them anymore. The mastermind who had sent some of the commands over the past few hours congratulated the team on the haul.

"Good job, everyone," he texted in the group chat.

That mastermind was Maximilian Rivkin, a gangster originally from Serbia who more commonly went by his nickname, Microsoft. He was a heavyset man with short dark hair that gripped the top of his egg-shaped head. Some gray had started to appear in his thin beard, which showed the beginnings of a handlebar moustache. On his right forearm, he had a large tattoo of the three wise monkeys from folklore that symbolize the wisdom of hear no evil, see no evil, and speak no evil. Microsoft did all three.

Microsoft was a true twenty-first-century drug kingpin: technologically savvy, globally connected, and capable of smuggling a variety of illegal narcotics from different parts of the world. He spoke an amazing array of languages: beyond Serbian and Swedish, he planned his crimes in Bosnian, Spanish, English, and, as he had shown during the speedboat operation, Croatian. Microsoft was "always online," he later told an associate in an encrypted text message. A workaholic, he sent encrypted messages nearly every moment of his waking life.

Microsoft was previously convicted in Sweden for serious drug offenses. At some point, he changed his name to Rivkin from his birth name of Milos Jankovic and jumped straight back into the game. Hard. At the time of the Swedish cocaine job, he told associates he was under house arrest in Belgium. Around five months earlier in December 2019, police had stopped Microsoft and an associate in the country. A Toyota Yaris the men were in reportedly had a hidden compartment. Authorities suspected the pair of being linked to cocaine trafficking. That encounter didn't stop Microsoft.

This speedboat operation was just one of a seemingly unending list of harebrained schemes Microsoft had for trafficking drugs. At various points he discussed, and sometimes succeeded in, shipping hash hidden inside

furniture, cocaine inside tiles, and more cocaine nestled among shipments of tulips. He told a conspirator he once secured a flight school's airfield in Denmark to facilitate a plane packed with product. To another he discussed setting up a legitimate vegetable company, including hiring a web designer, to then import food produce that he could hide drugs in. He controlled a timber company in Belgium that could be used for shipping goods to Ecuador. Another legitimate import useful for smuggling drugs was animal feed. At one point he had a corrupt insider at a factory that packaged energy drinks. That insider was prepared to hide precursor chemicals for making amphetamine inside the cans. He talked about having a sailboat for drug smuggling in Grenada, and spoke to a colleague about the cost of trafficking cannabis from Colombia. Now, the people Microsoft worked with in the midnight drop of hundreds of kilograms of cocaine wanted to do more jobs, including in Australia. "They have an endless number of ships," Microsoft told one associate.

That was a dizzying amount of business, but Microsoft stayed in his lane: when one person suggested he get into trading gold, Microsoft said he doesn't touch stuff he doesn't know about. He knew all about smuggling drugs, that was it.

The only thing that interested Microsoft was money, but he wasn't the best with numbers, even for an international drug trafficker. He sometimes kept such poor records that he had to ask co-conspirators to remind him how many kilos of drugs he had sold, and by his own admission math was his weak point. Where he shone was building a spiderweb of contacts. He was constantly juggling multiple international projects through his network of worldwide connections. He knew everybody, one associate said. In chat messages across various encrypted phones he mentioned the Hells Angels biker gang in Canada and Europe. In another, he suggested he had wide control over Antwerp, one of the busiest ports in the world and a notorious logistics hub for drug trafficking.

Microsoft didn't necessarily like all of the people he worked with, and often made racist comments in his encrypted text messages. When one Moroccan gangster was unable to work during the Islamic holy month, Microsoft texted in response, "Fuck Ramadan." He preferred to work with Albanians.

Microsoft was, obviously, a big deal. And he knew as much: he had now been trusted with the responsibility of handling the four hundred kilograms of cocaine coming into Sweden via speedboat.

Microsoft was also, quite simply, "crazy," according to multiple people who worked with him.

A year before organizing the plan to smuggle the Colombian cocaine into Sweden via speedboat, Microsoft was in Colombia himself. During a trip to Cartagena, a port city popular among cartels as a stop-off in smuggling routes, Microsoft went on a drug-fueled rampage through the Hyatt Regency hotel. As, authorities say, his body flowed with cocaine and ecstasy, then thirty-five-year-old Microsoft snapped and threw a chair out of a smashed window of his apartment on the eleventh floor. It crashed to the ground below, endangering passersby. He also hoisted a blender out of the window. And a table. And a broom. A crowd of people gathered on the street across from the hotel and shielded their eyes from the sun as they pointed upward at what was bizarrely unfolding in the sky above them. Microsoft's outburst was seen as such a danger that the hotel evacuated, as did a nearby supermarket. Eventually police and immigration personnel managed to take Microsoft to a nearby hospital. The medical center said the self-inflicted cuts and bruises were from his tirade.

Authorities later alleged that Microsoft had come to Colombia for sexual exploitation. He was there for the sex tourism. "It's not the tourism that we want to come to our country," the general director of Migration Colombia said at the time. For that and his rampage, Colombia wanted him out.

Police took Microsoft to Cartagena's immigration center, where they verified his identity and his Swedish nationality. Initially, authorities thought the man in front of them was American.

Officers transported Microsoft to Bogotá's El Dorado International Airport, a twenty-hour drive away, and made him fill out some paperwork to complete his expulsion from the country. Hunched over a desk in a drab processing center and flanked by two officers, Microsoft picked up a pen in his left hand, held it at an awkward angle as if he had trouble writing, and signed the papers. After the group of officers escorted Microsoft through the airport, Colombia banned him from entering the country for seven years. Realistically, he was lucky to get away with just a kick out the door.

Microsoft could flip from that sort of unhinged behavior, to saying that he loved his co-conspirators, to then threatening to kill someone. A colleague smirked that Microsoft had seven different personalities.

He had an encrypted phone for nearly each of those. His pockets were something like an operator switchboard, holding a Sky phone that he used to coordinate the speedboat haul, and a second Sky phone too. He at one point played the role of encrypted phone dealer himself and sold Sky devices in Sweden. Microsoft was also a customer of Encrochat—some of his contacts used that particular network, so he would have needed the same to communicate with them.

Microsoft hadn't added an Anom phone to this collection, yet. But something was about to shake the criminal underground that would force a migration of customers from one platform over to the FBI's secret startup. Microsoft would be going with them.

Act III

Chapter 16

Encrochat

Haroon Raza was in his living room in Capelle aan den IJssel, the Netherlands, on a coffee-fueled Saturday morning in June 2020 when he first read the earth-shattering news. Encrochat had sent a message to customers through its own app saying the company had been hacked.

"EMERGENCY FOR ENCRO USERS," the text message started, with simple black text on a white background. It claimed "government entities(s) [*sic*]" had taken over some of the company's infrastructure and used that to launch a hack against Encrochat devices. The five-alarm-level warning didn't go into specifics on what the hackers were able to get from Encrochat's phones, but it made the seriousness of the situation clear: it urged customers to immediately power off their phones and dispose of them.

"Due to the level of sophistication of the attack and the malware code, we can no longer guarantee the security of your device," the message to Encrochat's now-panicked users read.

Crimesite.nl, an independent website focused on the latest updates in the criminal underworld, paraphrased parts of the message for others to see. Who exactly was responsible for the hack, or what had been siphoned away, if anything, was still hazy.

Encrochat, like Phantom Secure, was another encrypted phone provider hugely popular among organized criminals, especially in countries that produced cocaine and laundered cash. Crooks flocked to its products specifically to avoid law enforcement surveillance. Now, it seemed the

police had not so much come knocking as driven a battering ram through each Encrochat phone.

Encrochat had around sixty thousand users, and Raza, learning of the news with everyone else, was one of the twelve thousand in the Netherlands. But Raza was not a criminal. Instead, he was a defense lawyer who happened to have gangsters among his clients. Raza owned an Encrochat phone to speak to those clients, some of whom simply did not use ordinary cell phones to communicate. The clients didn't trust generic phones even to speak to their own lawyer. Raza couldn't always travel to Turkey, Morocco, or Dubai to meet these people face-to-face. So, Encrochat was the only way to reach them.

After reading the news, Raza's immediate concern was for those clients. No matter the crime, organized crooks were still entitled to legal representation. The idea of attorney-client privilege, where defendants' communications with Raza should be free from surveillance, was a basic tenet of the justice system. Lawyers could not develop fair and effective legal defenses if authorities snooped on their deliberations.

And yet this news suggested cops may have hacked into every Encrochat phone they could, including those of some people not suspected of a crime, like Raza.

Raza and Encrochat's other users didn't yet know it, but the government entity responsible was the French Gendarmerie, a police department that is part of the country's armed forces. For years, Encrochat phones had appeared at the scenes of unrelated drug busts in the country. A gang that stole vehicles. A driver of a vehicle with a hundred kilograms of cannabis resin. Another group that imported heroin and crack cocaine from the Netherlands. They all used Encrochat.

The Gendarmerie, repeatedly stymied by Encrochat phones, started to investigate the company. Eventually the authorities found an Encrochat server was in their own backyard. This piece of key infrastructure, which also delivered updates to the phones, sat inside a commercial data center in Roubaix, France. That provided ample opportunity for police to then inspect the servers and figure out how the system worked. It was as if Encrochat had built a heavily secured door, able to withstand explosives and gunshots, but then left the key under the doormat.

The French police hijacked Encrochat's update process to secretly include within an application a bundle of the authorities' own code. This code silently tampered with the phones, including disabling the much sought after wipe feature. Most crucially, the update captured Encrochat users' stored messages. Where criminals felt most safe, and spoke most openly, the French military police listened.

From April 2020 investigators started by collecting the stored messages and then moved on to nearly real-time collection. Over the next few months, investigators gathered one hundred million Encrochat messages and shared the contents with police in the Netherlands. Hundreds of Dutch investigators then read the messages. Finally, police in the UK, Norway, and Sweden acted on the messages too, quietly arresting suspects.

Encrochat users felt something was wrong but couldn't put their finger on what. In pockets of Europe, the police pulled gang members off the street. The cops seemed to be everywhere the criminals turned. The users just couldn't figure out how.

"[The police are] all over it aren't they," one Encrochat user in the UK wrote to an associate. "My heads still baffled how they got on all my guys." The pair concluded there must be informants giving information to the police.

In May, some Encrochat users noticed the wipe feature wasn't working properly. They complained to Encrochat, who started to investigate. At the time, the company believed these users had simply forgotten the PIN number that triggers the wipe, or that it had not been set up correctly.

Then in June, Encrochat got ahold of one of the impacted phones. In the first sign that something was seriously wrong, the issues weren't due to user error. Encrochat found malware on the phone. Someone, somewhere, had hacked into it.

As Encrochat kept digging, it found the malware could do all sorts of things: it recorded the password that unlocked the phone, copied data from the phone, and communicated with a server controlled by the hackers.

Encrochat scrambled. Within forty-eight hours the company pushed its own update to customers' phones, in part to fix its users' issues but also to gather information and figure out what exactly they were dealing with.

The company's owners knew they were only buying time though. Given how sophisticated this attack was, they expected the hackers to strike again.

As soon as Encrochat's Band-Aid was installed, the attackers reacted. This time they hit even harder. Rather than only recording phones' passcodes, the new piece of malware introduced the ability for the hackers to change the passwords. The attackers could switch the locks on tens of thousands of doors at the click of a mouse.

Encrochat responded again by severing its own SIM card service, cutting off its customers from one another but also pulling up the drawbridge from the hackers. The company decided to go loud and on that June day sent the emergency message to its entire customer base. That was the message Raza read from his living room. The warning landed like a grenade in the organized criminal community. Encrochat customers threw their phones away in a futile attempt to destroy any evidence they held.

As well as sending the message to users, Encrochat contacted its SIM card provider, the Dutch telecom KPN. Encrochat explained that an attack was ongoing and asked KPN to block what Encrochat said were malicious servers. KPN obliged.

But within 160 minutes, KPN suddenly lifted those restrictions, and the hackers were back in.

Encrochat was all out of options. The company's bosses made a difficult, but immediate, decision: in an act of seppuku, Encrochat closed itself down.

"We have been forced to make the difficult decision to shut down our service and our business permanently," the company wrote in a statement sent to journalists.

As Encrochat pulled the power on its own network, the French police's collection of messages came to a sudden halt. The authorities had gathered a mountain of data, but their game was up. It was time to come clean.

Not before letting criminals squirm and speculate about what lay ahead, though. With related arrests across Europe well underway, crooks started to send one another court documents that included copies of people's Encrochat messages. People already in prison gossiped about what this might mean for organized crime across Europe.

On Thursday, July 2, around two weeks after Encrochat broadcast its warning, European authorities held a press conference and took responsibility for the hack. Attempted murder for hire, international drug

trafficking, extortion, narcotics laboratories—the small group of officials explained they saw it all.

"International drug and money laundering corridors have become crystal clear," Dutch authorities said in their press release.

Police found seven shipping containers inside a warehouse in Wouwse Plantage, a town on the Belgium-Netherlands border. Six of those containers had been set up as a makeshift prison. The final container was converted into what could only be described as a torture chamber. A dentist chair sat in the middle, with red restraints to lock the victim in place. The container walls were covered in soundproofing material. In the prison cells, handcuffs hung from the walls to tie people up, and a camera in the corner of each cell kept watch. Police were already investigating the gang connected to the cells but found that chamber after the Encrochat hack. Authorities also found police uniforms, handcuffs, and bulletproof vests (within two years, ten of the eleven suspects were convicted).

In the Netherlands, a nexus of Encrochat activity, police arrested more than a hundred people, seized more than eight tons of cocaine, found dozens of weapons, dismantled nearly twenty drug labs, and seized around twenty million euros in cash.

The biggest shock was likely in the UK, where authorities estimated up to ten thousand Encrochat users lived. Here authorities made nearly 750 arrests thanks to the data in the UK's biggest ever operation against organized crime.

Encrochat messages were full of English gangsters with their very English slang. They spoke of the "plod" (police); making sure to "flap" drugs (testing the product); "all gravy" meant the job was done. One UK criminal had the quintessential username CuppaTea on Encrochat.

Beyond the cheeky banter between crooks, the Encrochat data gave UK police a never-before-seen insight into drug trafficking across the island. Messages pointed to a senior manager and drivers from a trucking company who hauled tens of millions of pounds on behalf of other criminals. The drivers picked up cash from across the country then drove it to London. Later, the cash was sent elsewhere and laundered into legitimate businesses.

The messages took the police inside multiple million-pound cocaine trafficking rings. They exposed corrupt Royal Marine Commandos who transported drugs and ammunition and former professional soccer players

connected to the distribution of kilograms of cocaine. One Albanian dealer spoke about potential one-hundred-kilogram cocaine shipments and possible weapons trading. It emerged that his wife was a Metropolitan Police officer.

Guns, a relatively rare sight in the UK with its strict weapons laws, were all over Encrochat. Another gun runner stockpiled weapons including an Uzi, a scorpion submachine gun, an AK-47, and several different handguns.

It was easy to identify some of the criminals when they sent photos of their children or pets across Encrochat. For the National Crime Agency (NCA), the UK's version of the FBI, the hack was the law enforcement equivalent of the D-Day landings of World War II, one lawyer later said.

Soon after the hack, Raza contacted the Dutch National Public Prosecutors Office to provide his username on Encrochat. His hope was that investigators would filter out his privileged communications with clients. He had done this several times before with other encrypted phones from companies like Ennetcom when criminals used that platform. Raza stopped using such devices in 2019 when he started to suspect that police may be gaining access to their networks. He only grudgingly came back to using encrypted phones, and Encrochat and Sky specifically, because of the ongoing COVID-19 pandemic, which restricted his ability to meet clients face-to-face. Raza hadn't yet reported his Encrochat phone to the authorities.

"You are taking a risk by not reporting this until now, but that is of course entirely up to you," Evert Harderwijk, an official who oversaw investigations from the National Public Prosecutor's Office, wrote to Raza shortly after the authorities went public with the hack. Harderwijk told Raza the Public Prosecutor's Office had made his Encrochat and other messages "inaccessible." Later, though, Raza learned that Dutch authorities had continued to read some of his encrypted texts, despite him reporting the relevant encrypted phones.

In the way the French military police hacked Encrochat—indiscriminately and at scale—authorities put the onus on noncriminal users to make themselves known. The French military police did not know who owned each Encrochat phone—that was part of why they hacked the platform in the first place. But that in turn meant it did not know if their malware landed on the phone of someone not engaged in criminal activity, like a defense lawyer. The police hacked first, asked questions later. Or rather, forced others to volunteer answers themselves. French authorities estimated more than 90 percent of Encrochat users inside the country were engaged in criminal activity. That still left about 10 percent of people who were not.

That approach of walking through the dark extended to Anom in a way. Because of the organic marketing of the phones, the FBI did not know who was going to buy an Anom device until their messages flashed on a screen in San Diego. The agents knew there was a chance that a lawyer may end up using one of the phones.

"If an attorney got one of these devices, I've got no issue with that attorney, but we were going to do our best to make sure that we maintained the US stringent standards of monitoring," Kalina later recalled. That is, not monitor attorney-client privileged messages.

At least one lawyer using Anom allegedly fell into criminality. In Australia, authorities tracked one defense attorney who they claimed directed an associate to destroy potential evidence in a criminal case. But nothing about a lawyer using an encrypted phone indicated criminality in and of itself.

To criminals, the Encrochat hack showed them just how far law enforcement agencies were prepared to go to break into their encrypted messages. Hacking users on a worldwide scale was now a reality. What many of the crooks would not expect is that authorities would secretly run their own encrypted phone company. Encrochat's dramatic and sudden exit left a crater in the encrypted phone industry. Desperately looking for an alternative, many Encrochat users who hadn't been arrested now ran away from one trap straight into the claws of another: Anom.

Drum and bass music rumbled through the apartment while lines of text scrolled across Afgoo's screen. On a wooden dining room table sat a nearly perfect semicircle of fifteen phones, all plugged into a small black box.

"Finished. Total time: 0.335s."

"Finished. Total time: 0.329s."

"Finished. Total time: 0.017s."

Each line of text represented a new phone being loaded with Anom's software. This was Afgoo, and by extension the FBI, capitalizing on Encrochat's fall. The black box was like the one used by the Hong Kong electronics company to flash Anom devices. Now Afgoo took one of the boxes to Europe. By getting a massive stockpile of phones ready, Anom could jump on the Encrochat opportunity and grab new customers.

The fifteen phones on the dining room table were just one part of that stockpile. Next to the table sat columns of around ninety white cardboard boxes, bringing the total closer to a hundred. Videos shared among Anom sellers showed Afgoo's progress at prepping that inventory. But those sellers did not know the FBI was the one behind the push.

More organized criminals jumped on the chance too. They wasted no time in becoming brand ambassadors for the company. For Anom, Encrochat's death provided the best opportunity for growth yet.

Most of the time, Anom's sellers sourced hardware to then install Anom's software onto. In a handful of occasions, though, the San Diego FBI stepped in. When the phones needed to get to a certain location, or it was harder to source phones in a specific place, the shadowy figure of the FBI provided a helping hand. Without the knowledge of the Anom sellers themselves, though.

The music continued to blare as Afgoo flashed phone after phone after phone. Those phones were to be used to spy on more criminals. At one point, a dance track with a particular title played: "Sell My Soul."

Chapter 17

“We Move Anom Like We Move Kilos”

Just a week after police announced they were responsible for the downfall of Encrochat, Microsoft was crammed into an aisle seat in row fifteen on a commercial flight to Istanbul, Turkey. He was traveling to the city with Ivan Butina, a fellow convicted drug trafficker, who was in the other aisle seat across from him. During the flight Butina pulled up his Samsung mobile phone, framed a selfie of himself and Microsoft, and tapped the button. COVID-19 restrictions meant face masks covered both of the companions’ mouths—black for Butina, and red and orange flames on Microsoft’s—but their eyes were smiling.

Microsoft grew up under Butina in the crime world. The aging gangster had straight silver hair that parted in the middle and beady eyes. Microsoft held great respect for his elder and called him “uncle” even though the pair weren’t related. Both from Malmö, Microsoft said Butina was a living legend where he was from.

Microsoft had realized he was in a mess because of the Encrochat hack. He was one of the sixty thousand people who had used the company’s phones with their texts now potentially in the hands of law enforcement. Microsoft had used his Encrochat device to plan an assassination. That included sending photos and talking to people about traveling related to the hit. At one point, the Danish police warned the target about the plan, Microsoft believed. He suspected the authorities might have these messages, and, even worse, at one point he had taken a photo of his own

house with the phone. He had put too much trust into Encrochat, and now he had to live with that carelessness.

Despite that dire realization, Encrochat's death presented Microsoft and Butina an opportunity. Up until its closure, Encrochat was the most popular encrypted phone for criminals in Sweden. In the chaos of the company going down, space for a new player in the encrypted phone world presented itself. Plenty of criminals in Sweden and others further afield were now looking for a replacement device to secure their communications.

Finding that replacement was the reason for the pair's trip to Istanbul. They would get to know better the people linked to Anom, who would then explain how good the encrypted messaging platform was.

Butina wasn't in all of the meetings in Istanbul. When he had time he visited the Hagia Sophia Grand Mosque and snapped a photo of its ornate domed ceiling on his phone. Microsoft, meanwhile, met someone whom he later described as "the encryption king."

Hakan Ayik, the artisanal smuggler now at the helm of Anom's international expansion, wasn't going to stop at tasking just one phone seller to push Anom in Europe. Now Microsoft was getting in on the action too.

Ayik and Microsoft developed more than a business relationship; they became close. Two major drug traffickers now with a shot at running a large chunk of an encrypted phone company.

"I was at the table when the deal was made," Microsoft later recalled to an associate in an Anom message. "Anom will be the largest one in the world."

Sweden had a massive, and violent, organized crime problem. Gangsters executed people as they sat in barber chairs in broad daylight. Explosives detonated outside target houses ripped the doors off innocent neighbors' homes. During a four-year period that was reported in 2018, the country had the second highest recorded rate of deadly gun violence in Europe, with eight out of ten shootings connected to organized crime.

Outlaw biker gangs like the Hells Angels and the Bandidos had steadily increased their presence in the country since the mid-1990s and brought more drug trafficking and violence with them. Gangs targeted one another, and sometimes police were killed too.

As well as dealing drugs, some of the criminal groups made money by offering hitman-for-hire services. These hits weren't limited to within Sweden's borders, and some assassins traveled elsewhere throughout Europe to plan murders.

These were Microsoft's people and the community he wanted to tap for Anom. Ultimately, the goal was to cement Anom's presence in Stockholm and another Swedish area with what Microsoft estimated as thousands of potential users there.

Microsoft was a turning point for Anom. Up until now, the main seller in Europe had been Bobby, who at least projected himself as a legitimate businessman. From now on, that growth would be pushed in large part by a violent, international drug trafficker.

Microsoft and Butina returned to Sweden from their Anom meetings and immediately entered an encryption turf war. A handful of resellers battled for supremacy over the country's drug trafficking and murder-for-hire gangs. Among those were resellers of Sky phones. Sky was so popular, sellers joked that every other man was a Sky vendor. Microsoft claimed Sky products had been part of his networks for several years by this point. It had such solid brand recognition that some drug traffickers even went so far as to emboss the Sky logo into their blocks of drugs. Anom, meanwhile, was the unknown newcomer.

Microsoft built a team of a half dozen or so resellers and advocated for what he described as super geeky people to run customer support. Microsoft knew how demanding this job could be from his days reselling Sky, and he preferred to delegate the hard work to his underlings while he raked in cash from sales. The most important thing for Microsoft's sellers was that they kept their Anom phone in their hand at all times so they could be reached at any time of day.

The rollout was sloppy at best: Microsoft complained that Butina didn't push Anom hard enough, and Butina scribbled his sales on a piece of paper. He even roped in his daughter to handle customer support. Butina was drawn to selling Anom because he says he was told that the sale of Anom phones would be done entirely legally. Anom would be incorporated and sold publicly in shops. Maybe the company could even have an Instagram profile to generate publicity. Butina had recently served a long prison

sentence and had no intention of going back behind bars. Anom would be his way to generate income without having to resort to crime.

Microsoft shut down that idea nearly immediately. Anom was not going to be in phone shops under his watch. Sales were going to be completely underground, from person to person.

"We move Anom like we move kilos," he said. Butina was not going to get his stepping stone out of the criminal life.

Microsoft's first tactic was to outprice the competition. While prosecutors later said a Sky subscription could cost between $1,000 and $2,000, he offered promotions of Anom for as little as $600 in some cases. Microsoft went even further and gave away the phones to prospective clients for free. Worry about the money later, and take as many as you want. Just hand out the phones to your people, he told his gangster contacts.

The bargain bin prices worked, to a certain extent. Customers liked Anom's cheap cost but were skeptical of this new device on the market. Even by the fall of 2020, some didn't yet dare to use the phones for crimes. Some prospective customers wanted to be sure that the servers were located outside of Europe, meaning it would be more difficult for police to get hold of their messages.

Microsoft assured contacts that the police were not going to get anywhere near Anom. The guy behind the company, he believed, was wanted by the FBI, and "one of the most criminal people there are." Anom was "just me and other criminals there," Microsoft wrote in texts.

"You can trust Anom," he told Butina in one message, who said in response, "You know I can't trust technology." Demonstrating how much faith he had in the system, Microsoft sent photos of his own Swedish identification card, with his name, date of birth, and photograph across Anom. For him, Anom could safeguard such secrets and those of his potential customers too. Anom was the much better alternative. His staff boasted that Anom was never offline.

As customers trickled in, so did their requests for new features on the phones. One wanted the simple ability to change people's names in his contacts. Microsoft said he would compile these user issues and report them to Anom headquarters. He often annoyed the Anom support staff, rapidly and haphazardly flip-flopping between demands: take out the ability to contact support from the users' phones, then put it back in; introduce the

ability to make voice calls, and then he'd change his mind, again. Afgoo told staff to bear with him because he was such a huge influencer. When it came to tapping into international criminal networks to sell phones, Microsoft was second only to Ayik.

Microsoft's status as an international drug trafficker was part of Anom's appeal. Here was a successful and aggressive smuggler who vouched for Anom for his own drug deals. If that wasn't a ringing endorsement, what was? He knew as much himself and told others that with his influence and power, "people listen to me."

Microsoft seemed to truly believe in the product he was selling. Whereas police may be able to read your Signal messages if they catch you with your phone, he said, that was not possible with Anom. Anom was the solution that criminals were looking for. When Anom's own marketing didn't convince people, Microsoft played dirty. He went on the offensive against Sky specifically. He spread negative news stories about Sky that claimed the devices were vulnerable to hacking by the police. His staff stressed to others that Sky was based in Canada, which was part of the Five Eyes intelligence alliance. He told his resellers to steadily remove contacts from their own Sky phones. That way, more people would need to come to Anom. When one associate said they had two hundred contacts on their Sky phone and that it was difficult to migrate them all, Microsoft's response was to offer them two hundred Anom phones. There was a finite market for these criminal-focused devices, and Microsoft needed to squeeze customers from one platform to another.

"Only pussies use Sky, say that to them," Microsoft told his resellers. Being a criminal himself, the security of these devices was deeply personal to him. When an associate of his kept using Sky, he told them matter-of-factly, "This is my life, you understand."

"If you use Sky, you are also playing with my freedom."

Finally, when undercutting or undermining the competition didn't give Anom an edge, Microsoft had a third option: violence. He likened the selling of phones to having a drug territory: if someone else on his or his resellers' turf sold encrypted phones, he suggested sending someone to shoot them.

"There is too much shooting with you," Butina said. "Who says whose territory this is?"

“It is mine. Nobody sells but for my people,” Microsoft snapped back. “I haven’t even started yet.”

The FBI watched everything unfold from their desks in San Diego. As Anom became more popular in the criminal underground, the agents moved from room 2415 into a larger space next door. They set up yet more rows of computers and sometimes borrowed monitors from the desks of other agents who were still not in the office due to COVID-19. When more analysts joined, each went through an onboarding process where they were taught a lexicon of various syndicates’ slang terms. When they needed more space for more analysts, the FBI dismantled partition walls separating their space from the next, making their wire room larger and larger.

Given Anom’s now international reach, the FBI sorted the space into geographical regions, with agents focused on certain countries working in different parts of the room. The FBI roped in translators who hurriedly typed the messages into English. They also used machine translation tools from Amazon to quickly summarize what was being said.

The work continued to ramp up. The agents worked sixteen hours a day, reading messages late into the night. The linguists worked long hours too. The FBI ordered pizza for agents reading the Anom messages. Management told them to grab a slice and get back to their computers.

The best part of Anom’s expansion was that agents didn’t even need to do any work to sell the phones. Criminals like Microsoft and his customers did the heavy lifting for them.

“We allowed these devices to be sold organically across the world,” Kalina later recalled. That hands-off style was important: if the FBI sought out a specific person and sold them a bugged phone, that might be a legal issue. “We never made a decision to approach anybody individually. Because we knew that would be an issue of entrapment,” Kalina added.

A high-ranking criminal would buy phones from Anom and then turn around and sell those phones to other criminals, either at a markup or for a slice of the profits. The structure was exactly like what the FBI had seen work so effectively with Phantom Secure before it. The organic distribution model became “a cycle that feeds itself,” Muse added. “They want to sell more phones, so that they can earn more money on their sales, get more phones in more hands, and it grows exponentially from there,” he said.

To Kalina, it was more than a marketing approach. Anom was a pyramid scheme. At the top of that structure was the FBI. Money from the sale of Anom phones trickled up to the FBI, which then funneled some of that cash back into running Anom, such as buying phones when necessary or secretly paying for the infrastructure. Kalina said, “We were creating our own pyramid scheme amongst the criminal world. And better believe it, they took advantage of it.”

Chapter 18

“Let’s Make Millions”

Reece Kershaw, the head of the AFP, walked up to the wooden podium on the stage on July 22, 2020, several weeks after the shutdown of Encrochat. Dressed in his formal police uniform with medals adorning his chest, having entered the job less than a year earlier, Kershaw provided an update on what the AFP would focus on under his direction: foreign interference, counterterrorism, transnational organized crime, cybercrimes and fraud, and child exploitation.

Kershaw also had a message to relay as he spoke into the two small black microphones. The message wasn’t for the people of the National Press Club of Australia, though. It was for Australia’s organized crime figures.

“We will be relentless. We will outsmart you. And we will always be a step ahead. The full force of the Australian Federal Police is coming for you,” Kershaw said. Some in law enforcement could take it as a veiled reference to the phone-shaped spy inside Australian criminals’ pockets, the one that the criminals had no idea was actually bugged.

Anom now had a network of distributors spread across Australia, similar to how Phantom Secure created the blueprint for selling phones in the country years earlier. One too-enthusiastic Anom seller made a rookie mistake. When preparing promotional messages to send out to potential customers, they claimed that Anom was “designed by criminals for criminals.”

Other Anom members flipped out. Such a statement was asking for trouble. Of course, generally the phone sellers and the higher Anom staff

knew that their clients were criminals. Quietly serving criminal customers was one thing; explicitly acknowledging your service was for the benefit of gangsters was another. The criminal user base was a taboo topic among some of the staff. One Anom worker got so used to repeating a line of boilerplate text to anyone who inquired about crime that they became very quick at typing it. Anom's workers were not going to make the same mistake as Ramos, who essentially admitted that his phones facilitated drug trafficking. The text read, "We do not condone nor encourage the use of the Anom network and devices to commit any crime."

If organized crime groups in the country took any notice of Kershaw's ominous speech once it was published online, they didn't show it. Catanzariti, beyond providing Australia's underbelly with Anom phones, had better things to do. Around the time Kershaw stood on stage, Catanzariti was busy smuggling a shipment of cocaine worth around $20 million AUD. He had moved on from chatting about Batman, as Muse saw from San Diego. This time, the cocaine blocks were stamped with the text "Jaguar" and the luxury car brand's logo.

Catanzariti wasn't masterminding the whole operation. Instead, he was helping out some conspirators. In late August nearly eighteen kilograms of cocaine, shipped from Greece via air, landed in Australia. The drugs were hidden inside a crate containing a pair of Technomig 3000 welding machines. The smugglers had been sloppy and left the necessary paperwork to push the consignment through to the last minute. The machines now sat in border purgatory in a section of Adelaide airport. Catanzariti needed someone to clear the shipment through customs.

On Anom Catanzariti chatted to a professional customs logistics expert, a bald, heavyset businessman called Silvio Molinara. Catanzariti stressed to his contact to limit all communication between them to the encrypted devices.

"No fones please. Lol just this," Catanzariti wrote.

Despite his white collar employment, Molinara leaned into Italian gangster stereotypes in posts on social media. He uploaded memes of *The Godfather* and *The Sopranos*, with text like "those who want respect, give respect." Molinara was a director of one Australian section of Standard and Partners. The company imported coal from Indonesia and South Africa, and also imported seafood, poultry, black truffle butter, and rice and soybeans. That access to the logistics industry meant it often flagged consignments through customs. Catanzariti needed Molinara to provide the paperwork and pay the relevant taxes that would get the welding machines out of the airport. After that, the rest of Catanzariti's gang could extract the cocaine stored within.

"They said its [welding machines] already here they just need an agent to clear it not bring it in," Catanzariti explained on Anom.

"All good bro. We need to lodge the docs. Pay the fees etc," Molinara replied.

"So does this affect u at all or u do this shit for people all the time," Catanzariti asked.

"We can do this dont stress," Molinara said.

For clearing and delivering the welding machines, Molinara would get a $40,000 fee. "Just get it happening," Catanzariti wrote.

Catanzariti knew the welders contained cocaine. He deliberately kept that information from Molinara—to Catanzariti, $40,000 was a tiny slice of what the potential profits could be. At wholesale, police would later say this amount of cocaine could sell for $5 million AUD. On the street, it could total up to $20 million AUD. But Catanzariti acknowledged that Molinara's professional services were key to anyone getting any money.

"Looks lets be relasistic [*sic*] he just signed off [unknowingly] on 18 keys lol. So of anyome should get paid its him," Catanzariti texted an associate on Anom. Believing that customs had been sorted, the crew inched closer to having the cocaine, and some of that money, in their hands.

"Ok lets make millions," Catanzariti wrote to his associates.

Catanzariti's bold smuggling scheme showed just how deeply involved Italian organized crime was in Australia. The AFP also started to gain a deeper understanding of the Calabrian Mafia, named after the region of Italy that its founders heralded from more than a century ago, and one of the most powerful crime groups in the world. The Calabrian Mafia had its tentacles all over the planet, and the AFP said it handled 70 percent of the world's cocaine. Members were loyal to one another and bonded by family blood.

Catanzariti shipped Anom phones to Italy, and the AFP believed Mafia members back in the homeland were the ones directing their underlings across the world in Australia. The group's Australian members had always been resistant to law enforcement penetration due to the code of silence among them. But with Anom, the members didn't know they were inadvertently talking to the cops. They spoke openly on the platform, where their digital whispers could be overheard.

The Calabrian Mafia may have been an ancient institution with more than a hundred years of tradition, but it still lived in the twenty-first century. It faced the same reality of sophisticated law enforcement spying techniques that other gangsters did. They needed to use encrypted communications just as much as any other top-tier organized crime group, perhaps even more so.

The group was sorted into clans, with members sometimes following a set of rules handed down through generations of families: keep a low profile and don't flash your cash, but don't be afraid to use violence or corruption. In line with that goal of staying under the radar, members used legitimate front businesses to launder the profits from their drug trafficking and other crimes. They were good at it: the Calabrian Mafia are believed to have been laundering cash in Australia since the 1970s. The AFP found agricultural, restaurant, and construction companies took dirty money in one side and pumped out clean-looking revenue on the other. Mafiosos controlled swaths of property with holding companies or in the names of their wives. The AFP found they used corrupt lawyers and accountants to give their income a convincing facade. The Calabrian Mafia hid in plain sight and effectively blended into the everyday fabric of the Australian economy. As well as its use of encrypted communications, the Mafia's

money laundering had evolved with the times too. Some members used the pseudo anonymous digital currency Bitcoin, the AFP found.

The AFP identified fourteen Calabrian clans in the country. The clans collaborated with other distinct criminal groups, such as organized crime groups from Asia or the Middle East. As Mafia members joined Anom, the AFP's insight on Italian organized crime ballooned from the Calabrian Mafia to the wider ecosystem of Italian organized crime clans in Australia. In all, the AFP found fifty-one such groups. Astonishingly, these clans were potentially the same size as Australia's biker gangs: some of the Italian groups involved thousands of members. It was as if a second, similarly sized criminal network was there the whole time, invisibly interwoven into Australian society, but its true reach was becoming clearer. Australian authorities of course knew Italian organized crime had a heavy presence in the country. But now the AFP was able to see just on what sort of massive scale.

Most importantly, both of these menaces—one overt with the bikers, one more stealthy with the Mafia—regularly worked together. The Italian clans, who provided much of the financial backing for the networks' crimes, outsourced violence or drug smuggling to the bikers. The Mafia controlled the bikers, or at least a lot of them.

On September 1, Catanzariti and the rest of the crew realized something was up. At about 2:10 p.m., another member tasked with picking up the machines walked into a white warehouse near the airport. He told staff he was there to take the consignment now that the proper payments had been made. Staff pulled up the shipping records and found something was off: the machines had been seized, they told the crew member.

Unbeknownst to the gang at the time, the Australian Border Force (ABF) had already found the cocaine. The day before, officers from the ABF examined a wooden crate. Inside that were the two welding machines. Then nested among both of those were two safes. A key was inside the shipment, and the ABF officials used it to open one of the lockboxes. Nine

packages of white powder were tightly packed inside, secured in clear film and tape. Later, AFP forensics experts closely examined the haul and opened the second safe. They removed the packages and performed a drug test. The powder was cocaine, 17.96 kilograms in total.

Over the next several days, the crew member sent a flurry of emails and returned to the warehouse to try to get what they said were their welding machines. It was futile. The machines, and the cocaine, were gone.

Catanzariti thought he knew what would happen next. The police, inevitably, would arrest the crew member who was supposed to pick up the machines. He was "like a sitting duck," Catanzariti texted across Anom.

Often when authorities grabbed some drugs, arrests followed swiftly after. But that didn't happen. By now, the welders had been on the ground in Australia for more than a week, and no one had raided the crew member's house. He hadn't noticed any heat.

Catanzariti thought the police might be taking their time with replacing the cocaine inside the safes with dummy materials. This was an approach police sometimes used to catch people picking up what they thought were drug shipments but actually contained innocuous substances. Another option, Catanzariti believed, was that the shipment had in fact been cleared, and it would be ready for pickup tomorrow. Or, maybe the AFP was following the crew member, to lead them to the other smugglers.

"Feds probaly watchin ythis guy see what he does," Catanzariti wrote.

The AFP did not need to follow the man who was supposed to pick up the cocaine. The police were already sweeping up Catanzariti's messages about the seizure. Letting the chats play out could have its benefits. Why shut people up when they're incriminating themselves over and over?

Eventually, the AFP broke that silence with a bang. On the morning of September 8, nearly two weeks after the shipment arrived, the AFP raided the crew member's house and arrested him. In their search of the house, the AFP didn't find any clothing or tools that would suggest he was really in the welding business. What they did find was a printout: an email including a picture of a Technomig 3000 welding machine. The same brand Australian authorities had just pried open and found contained eighteen kilograms of cocaine.

"Hey he got done," an associate wrote.

"What happened?"

“Pigs grabbed him.”

None the wiser that their messages continued to flash on screens in the Bunker, the group kept chatting in the aftermath of the arrest. Demonstrating the immense wealth some of them had, one member of the Mafia clan said they would give the arrested smuggler a house once he got out. The Mafioso also said he would pay the member’s rent and give his son financial support while he was locked away. It was already clear that the busted crew member was going to end up behind bars, and helping his family was one way to ensure that he kept his mouth shut. Other members wondered if they might be the next target of the AFP, which would “come knock my door off the hindges.”

The bust of Catanzariti’s associate and the seizure were one of Operation Ironside’s first successes. They proved the bugged Anom phones could lead to tangible results. The bust showed that Anom’s secret surveillance capability was more than letters appearing on a screen. Anom could be leveraged to track down drugs and people.

When the ABF and AFP announced the arrest the day after, the press release made no mention of Anom. Instead, it said that ABF officers “selected” an air cargo consignment for examination, and then they X-rayed the wooden crate and found anomalies.

In the same way the crew used the welding machines as a cover, the authorities had a useful piece of misdirection with the X-ray. Maybe the ABF would have found the cocaine anyway, but the secret monitoring of Catanzariti’s and others’ messages provided ironclad intelligence on who was pulling the strings of the shipment. The impacted crew might focus on the X-ray being the reason for the seizure. That was the impression a reader of the press release would come away with anyway. If that was the case, the criminals could keep trusting the Anom phones.

This was the constant tension underneath Operation Ironside: how to balance when to strike, and how to frame those raids, while keeping the ultimate source of the intelligence confidential. If the AFP grabbed too many people, it might become obvious that Anom was the culprit. But remain completely passive, and large quantities of drugs, or worse, would flood the streets.

The long game, of silently gathering intelligence on how organized crime worked as Anom grew, was more important than immediately

arresting every suspect, the AFP decided. They only attempted to intervene when there could be some plausible deniability on how they stumbled across the drugs, or when there was a clear threat to life.

The decision was much easier when weapons were involved. Earlier that year, Australian cops used Anom to pinpoint the suspected location of a Comanchero cache of weapons. Police found the military-style guns stashed in a hidden compartment of a truck.

Through Anom, the AFP continued to learn the smuggling techniques of the country's organized crime groups. Seven months before that weapons seizure, specially trained divers from the NSW Police were in the waters of Port Botany in Sydney. Botany was the largest container port in the state, which saw ships come and go twenty-four hours a day.

Underwater, the divers were in complete darkness apart from the small flashlights two of the officers held. After the divers stealthily swam to the hull of a docked container ship, they pointed those flashlights to a certain spot. A web of metal chains held a tire to the ship. As bubbles from their scuba gear steadily rose to the surface, the divers fiddled with the chains until they came loose. Inside the tire, a group of drug traffickers had hidden thirty kilograms of cocaine.

But the cocaine wasn't there. The Australian authorities believed the cargo fell out at sea before the ship reached the port.

This was the second time the drug traffickers' plan had failed. In October 2019, the smugglers imported another thirty kilograms of cocaine. Except that time, one of the criminal group's own divers dropped it to the ocean floor when he tried to retrieve the tire from under the ship. Their criminal handlers were furious.

The police knew exactly where to look for the chained-up tire because the importation was organized in messages fired across Anom. The AFP took that intelligence and arranged for the NSW divers to take a look. The divers didn't find any drugs, but the AFP could keep monitoring the smugglers' messages and see if they tried it again.

Operation Ironside was no longer just a few officers in the Bunker with computers. Now the operation reached out and touched the real world that the Anom messages echoed. Police quietly picked some weapons off the street and monitored drug organizations here and there. As the amount of intelligence increased, the AFP decided to brief more officers on what was

going on with Anom. They farmed out acting on the intelligence to Australia's regional police forces around the country. South Australia state police officials were brought into the loop. The AFP told them, in essence, we have all of this data because we're not just inside Anom, we are Anom. Still, the secret was kept limited to select officers. Bosses had to hide the source of this trickle of intelligence from even their own detectives.

Kershaw was right in his speech: law enforcement was one step ahead of the country's organized criminals. The criminals just didn't know how. To them, the seizure of Catanzariti's cocaine, and the increased frequency of other small police actions, could have been for any reason. Maybe someone squealed. Perhaps a smuggler made a mistake. Or the cops got lucky. The criminals were safe; their messages were encrypted by the best up-and-coming underground phone on the market. Or so they thought.

Chapter 19

Wasta

Dubai was where criminals went to avoid the heat. During the Istanbul meeting with Ayik, Bobby said he would take Anom to the big decision-makers in Dubai. Now mid-September 2020, Bobby was here, navigating the sweltering Dubai sun. Bobby was already professionally and personally intertwined with the city. One of his companies that sold encrypted products was incorporated there. In Dubai's cafes he hung out with employees, worked on his MacBook, and smoked sheesha while watching *House of Cards*. Bobby went to Dubai on holiday with his family and snapped photos of his wife posing in front of the city's iconic Burj Al Arab hotel. He uploaded many of these to Facebook. As Bobby started to work for Anom, he stopped sharing on the social network. The flow of happy family photos suddenly disappeared.

Dubai was unusual in that encrypted apps were illegal in the United Arab Emirates. The government held a tight grip on which communications tools it allowed to operate in the country. No Skype, Google Hangouts, or WhatsApp—they were banned for not letting the government monitor users' messages. And likely no custom phones that promised to be impenetrable to law enforcement. That didn't really stop a heavy concentration of Dubai-based kingpins from using the phones, but get caught selling one and you could face potentially serious penalties, even jail time.

Bobby offered exactly that sort of product. He brokered phones in the city on a decent scale. In all he sold around three hundred encrypted

devices. Bobby managed to sneak them into the city because he used a business mailbox at the airport.

Then Bobby's plan went off the rails.

Those sizable trades drew the attention of Dubai police. In recent days local authorities had swarmed around his phone business: First, Dubai police arrested Bobby's business partner for selling encrypted devices. In the wake of that bust, Bobby told an Anom worker to wipe the partner's phone. Then the cops raided Bobby's office in the city and seized his inventory of Sky and Anom devices. Those phones were not going to end up in customers' hands any longer, and the seizure hamstrung Anom's Middle East expansion.

Now Bobby worried he might be the police's next target. Other Anom workers told Bobby not to go looking around for his lost partner. Maybe it was better not to annoy the local police. Bobby ignored their advice and went digging.

Dubai's hive of traffickers made it an attractive market for phone sellers. All around the globe, foot soldiers guarded drug safe houses, cooks spun up batches of methamphetamine, and smugglers carefully packed blocks of white powder into fruit or other items. Many of their bosses sat in Dubai.

With so many expat criminals based there, Dubai was a playground, a safe haven, and a business opportunity all rolled into one. Some top gangsters in Dubai banded together to make so-called super cartels. These cartels crossed ethnic and cultural divides. Balkan mobsters worked with Dutch-Moroccan cocaine traffickers. Italian mafiosos teamed up with Irish gangsters. Then all of them came together as one.

What cemented all of the audacious behavior was the Dubai culture of *wasta*, an Arabic term that loosely translates to authority or power. On the surface Dubai is a highly authoritarian place to live, and for the vast majority of people, especially women, it is. But in the underbelly of Dubai, the more money you had the more wasta you could throw around and be allowed to live and act with impunity. And, obviously, the drug traffickers

who fled to Dubai had lots and lots of money. They lived in complete opulence. They bought sports cars, beachfront villas, and penthouse apartments, luxuries that might have already been seized back home. Life in Dubai might even beat living in whatever country they ran away from.

Dubai was where money got you nearly anything and the police traditionally left foreign organized criminals alone. The city asked for no personal income tax, and Dubai's real estate market was a perfect parking spot for the dirty money of drug traffickers and Russian oligarchs.

From those glass skyscrapers and fancy resorts, the gangsters used encrypted phones to remotely control their trafficking operations. No longer did they have to arrange face-to-face meetings. That took time and could lead to their capture. With the phones, the bosses' empires grew securely and uninterrupted. They often juggled devices to handle different pillars of their organization—packaging of the drugs on one phone, and laundering of the proceeds on another.

Anom had a shot at converting some of those criminal executives over to its platform. In turn, those high rollers would need phones for their underlings to send commands to. Anom could target the top players and then let the phones trickle down the totem pole. The FBI, conveniently, could piggyback off Anom sellers' aspirations and tap into this vibrant community of organized criminals.

By 2020, cracks had started to appear in Dubai's reputation as a safe haven for crooks. In July that year on behalf of law enforcement, Dubai authorities arrested two Australian kingpins who had fled the country. The Dubai police boasted about this bust by producing a slick, action-movie-style trailer of the arrest. Drone footage purportedly of a car chase was interspliced with flashy graphics and the targets' mug shots. If Dubai was finally going to shake its image of being a criminal safe haven, the government was going to be brash about it.

Dubai police had earlier arrested Ridouan Taghi, a notoriously violent drug trafficker who law enforcement said nonchalantly ordered assassinations of his rivals and was the Netherlands' most wanted man. The tally of busts for the benefit of international partners ramped up into the dozens.

Then, on September 15, 2020, around the time cops cracked down on Bobby's encrypted phone business, Dubai authorities arrested another major

trafficker called Denis Matoshi. Matoshi was said to be a leader of an Albanian crime syndicate called Kompania Bello, one of Europe's most active cocaine trafficking networks. The group had managed to weasel its way into the international cocaine arena despite Albania itself not being a producer or much of an end user of the drug. Encrypted phones allowed groups like this to expand geographically. With secure phones that had unlimited data SIMs, criminals were free to roam the world. Kompania Bello globalized its business.

The crew's ringleader had for years been trapped inside an Ecuadorian jail cell. That didn't stop him. From there he used encrypted phones to coordinate with his underlings in Belgium, Italy, and Albania. He used encrypted messages to communicate with associates who had direct ties with the South American producers and Central American cartels to arrange the massive shipments of cocaine.

This meant that Kompania Bello, very unusually for a drug enterprise, controlled nearly the whole supply chain. Its members sourced drugs from those producers in South America, safely transported them to markets, and handled distribution once the drugs arrived in Europe. Usually a syndicate handled one, maybe two of those. Kompania Bello did it all.

Italian state police led the investigation into Kompania Bello, and Dubai authorities arrested Matoshi on their behalf. Other law enforcement agencies detained nearly twenty wanted members at the same time. In its Facebook post announcing the arrest, the Dubai police made it clear that their city was not a safe hiding hole for criminals any longer: they said they had extradited fifty-two internationally wanted people in all, related to various investigations. Dubai looked less and less like a gangster's paradise.

Given the nearly simultaneous timing with Matoshi's arrest, multiple Anom workers believed the clampdown on Bobby's phone business was connected. Kompania Bello used Sky phones—Bobby had a bunch of those in his office, after all—and Encrochat devices.

Then things got even worse. About a week after the arrests, someone else contacted Anom to in turn wipe Bobby's phone. Puzzled as to why this outsider wanted to factory-reset a reseller's device, Anom staff talked among themselves about what to do.

Through these conversations it turned out that when Bobby continued to search for answers on what had happened to his employee, the Dubai

authorities detained him too. Officers lifted Bobby into a vehicle with blacked-out windows and pulled a hood over his head. To the outside world, Bobby vanished off the face of the earth. Anom's staff wiped the phone.

The Anom staff didn't know exactly where Bobby was, but one of Anom's key distributors now sat in a jail cell. With no seller and no phones, the company's Dubai expansion slammed to a halt. As did part of Anom's European rollout, which also involved Bobby. By arresting Bobby, the local authorities had unknowingly butted heads with the FBI's secret surveillance operation too, just as it was getting closer to tapping more top-tier organized criminals. Anom, the FBI, and the AFP would have to wait to get Anom's phones into the hands of Dubai's playboy gangsters. An Anom worker saw the situation for what it was: "a complete mess."

Despite Bobby's arrest, Anom did manage to sell some phones in the city eventually. The Australian police even got a stroke of luck. The phones landed in the hands of two specific senior bikers Australian authorities hoped to yank back home from Dubai. Police claimed they both had links to the Lone Wolf motorcycle gang. NSW Police estimated Benjamin Pitt and Matthew Battah were tied to operations that may have smuggled a staggering seven tons of drugs into Australia. They controlled the imports from Europe and Africa. Anom might help track them down.

The alarming thing was these two gangsters had already been arrested. They were the two drug traffickers the Dubai police had arrested on behalf of the Australian police two months prior. Pitt and Battah weren't using the Anom phones to traffic more drugs. They were using them to break out of Dubai's Central Prison in Al Aweer.

Dubai's prisons had a reputation for torturing inmates. One British prisoner claimed in a witness statement that police electrocuted his testicles during an interrogation and then forced him to sign documents written in Arabic at gunpoint. Pitt and Battah, obviously, wanted out.

As Australian officials read Pitt and Battah's messages, they could see right into the pair's thinking. Their plan came into view. The men

reportedly intended to first somehow get themselves to the prison hospital. From there, they would break out of the prison itself. Pitt and Battah were spending a ton of cash to try to get out. Wasta could get you anything.

"There was a significant attempt to break these people out of jail," Stuart Smith, the assistant commissioner from the NSW Police, later said. "We took the threat seriously."

At that point, Australian authorities shifted their operation. This was no longer a case of quietly waiting for the extradition process to run its course. Australian police contacted their Dubai counterparts, who then grabbed two phones from Pitt and Battah. The prison locked them down into maximum security. Anom now showed that the Australians could foil plans beyond even their own borders, and Anom let them reach across the world.

Weeks and weeks dragged on with no sign of Bobby. Eventually, an Anom worker received a message: "G'day." Bobby was finally back.

Dubai prosecutors had alleged he had been "selling and offering illegal telephones without a permit." The issue was specifically his sale of Sky phones.

"Me and my partner are free.… They just fined me hefty for selling Sky in Dubai," he texted an associate over Anom in Dutch once he was out.

He was released by the end of the year, at which point he celebrated in Dubai with his young children and wife. He was back on Facebook and live-streamed fireworks cascading over the beach from a high-rise. Soon after, he rejoined Anom with a different alias. He still worked under Ayik, but things were different: Bobby later claimed he was threatened and intimidated into continuing to sell Anom's phones. He gave in and bought more of the devices but said he didn't sell them on.

In all Bobby spent months inside Dubai's prison. While that was a roadblock for Anom's Middle East aspirations, it also impacted the company's European road map. Bobby was primarily focused on growing Anom on that continent. With him behind bars, that expansion stalled too.

Bobby wanted Anom to have an air of legitimacy. That plan vanished when he was arrested. The people who took charge of sales while he was gone had no intention of going legit. Microsoft was a drug trafficker, not a tech salesman. The gap in Europe presented a chance to seize more territory. Microsoft got aggressive.

Chapter 20

The Bridge

From summer 2020 onward, Mike Bobbitt was used to getting late-night phone calls from Cheviron about all sorts of crimes. Bobbitt was the FBI's assistant legal attaché in the Netherlands, the person who acted as a conduit between the FBI and Dutch law enforcement. The FBI stationed these agents all over the world to work with other law enforcement agencies.

There was only so much the FBI could do from its base in San Diego. For there to be any sort of actual impact from the constant stream of intelligence, the FBI had to pass information to foreign countries where Anom's users were based. One of the hot spots was the Netherlands.

Cheviron would often call Bobbitt with details on a new Dutch shipment or threat in the Anom messages. Bobbitt would then work with his Dutch counterparts to funnel that intelligence to where it could be best used.

In one case, Cheviron phoned at nine p.m. about what appeared to be a kidnapping plot. Through Anom messages, a gang leader was planning to snatch one of their previous transporters, the people who ferry goods around. Bobbitt opened his laptop at home and dug through the relevant chatter. The messages showed the area of the country the plot might unfold in but not much more than that.

Bobbitt passed along what he could to his Dutch contact, worked with them to get the intelligence to Dutch tactical units, and went to bed. At 2:30 a.m., Bobbitt's phone rang. It was Cheviron, again. The San Diego team had found more information: the kidnappers had put a tracking device onto the target's car, which was in a parking lot. The gang had its own static car with

a camera they were watching the area with too. The plan was that when the target backed out of the parking lot, the kidnappers would grab him.

With enough information to warn the target, Bobbitt woke up his Dutch contact, and the pair came up with a ruse. They crafted the intelligence in such a way that it looked like it came from an informant rather than the FBI's secret wiretapping of Anom. With that information, police warned the soon-to-be kidnap victim. He claimed he didn't care; his brother, who may also have been targeted, asked to go into protection. Dutch police ultimately found the tracker on the car.

That was just one of at least a dozen episodes where Bobbitt helped Dutch police with ever increasing tips from Anom. And each time, they kept Anom's connection under wraps. When grabbing criminals' weapons, the operation was framed in such a way that seizures looked like random traffic stops.

The number of Anom users in the Netherlands was growing into the hundreds, with some of the most important syndicates swept up in Anom based there. Which meant more messages for the FBI to translate and scan for threats to life. "It was just sheer volume," Bobbitt later recalled.

The Dutch had proven, again and again, they could be trusted with Anom's sensitive intelligence. So Bobbitt told Cheviron the FBI needed to give the Dutch access to Hola iBot themselves as soon as possible. The Dutch police would be able to monitor Anom's messages from the Netherlands themselves. Cheviron agreed.

So started the next phase of Operation Trojan Shield, with the FBI offering Hola iBot access to a tiny selection of trusted countries. Anom ballooned from an FBI and AFP project to one now involving European police too.

That phase came tragically too late for some.

Sascha arrived at the bridge in Stockholm, Sweden, in September 2020 thinking he was about to celebrate a friend's birthday. A short while later Sascha would be dead, lying on that bridge in a pool of his own blood, betrayed by some of the last people he trusted.

Sascha, dressed to beat the Swedish weather in a gray hoodie, Gucci sweater, and black outer jacket, got to the bridge around midnight. The bridge stretched across the bay Ärstaviken over a small island with a

historical farm and nature reserve. From the north bank of the bay, the pedestrian path headed toward central Stockholm.

Sascha was there to meet Toj, an old-time friend who invited Sascha over Snapchat to celebrate his birthday, and Kevin, another man. As the group walked along the pedestrian section of the more than eight-hundred-meter-long bridge, on one side was a fenced-off train track. On the other, past a gray metal railing, the dark water of the river Ärstaviken. Tall residential towers lined the bank. Apart from a couple of cyclists who rode past the three men, the area was deserted.

Sascha's life of crime had pushed him on a downward spiral. The previous year, Sascha was shot multiple times, first in October and then later again in the winter. Sascha survived but essentially ended up in a coma for some time. Sascha knew his life was likely in danger after those earlier shootings. By May 2020, a Swedish police officer phoned Sascha and told him as much. As is common in the criminal world, Sascha said he didn't want to receive any help from the authorities. But he kept a red-handled knife in his waistband for protection. Knives and bullets were how young criminals sorted out their differences in Sweden.

His violent life meant he drifted away from his mother, who felt they lived in separate worlds. There were moments of safety: earlier that day, Sascha and his sister Natara had a quiet evening doing the laundry. Broke, Sascha had so little money that one of his sisters ordered him a taxi for $10 to the pedestrian path to meet his friends.

Those friends, it turned out, could no longer be trusted.

On the bridge, one of the men pulled out a 7.65 mm caliber weapon and pointed it at Sascha's head from a close range. His hoodie provided no protection from the first bullet. It careened through Sascha's right cheek. Blood splattered outward.

Miraculously, Sascha was still alive. He tried to escape from the attackers and headed north along the bridge as a trail of blood dripped from his face. The rest of the long bridge stood in front of him. Sascha had to make it across the entire structure if he had any hope of getting away.

The gunman took aim again and fired three more shots into Sascha's back. Two of the bullets lodged inside his body; the third flew out the other side. Sascha fell. While Sascha lay on his back on the bridge, one of the men came over. He fired a final shot into Sascha's temple.

A computer server more than five thousand miles away across the Atlantic Ocean saw all of this coming. The entire killing—from sourcing a gun, to arranging payment for the murder, to discussing how and when to kill Sascha—was documented in the cold static of an FBI hard drive. The murderers planned it all on Anom.

Weeks earlier, Sascha's killers shared a photo of their target in Anom messages. Sascha's back was to the camera, but someone handily drew a large red circle around him on the picture. He was the target. The killers discussed using binoculars and a radio to spy on Sascha and find out where he slept. They organized where to leave ammo for the shooter to pick up later. One said Sascha trusted the group—Sascha didn't even wear a protective vest when they met up for food the month before the murder. One of the killers said he wanted to practice with a certain gun beforehand so he wouldn't miss. They plotted how to lure Sascha to a secluded spot, because he often moved around with multiple people, and to burn their clothes once the hit was done.

"We're doing it on Friday bro, the Swede," one of them wrote earlier that month, using their nickname for Sascha.

"We will reward you greatly," one of the organizers replied.

"Ok bro it will be Friday or Saturday, have to go tomorrow and plan," was the response. If the opportunity arose, they also plotted to take out Sascha's brother, Makael, at the same time. The night before the killers eventually lured Sascha to the bridge, one wrote, "Tomorrow we have him bro."

After the killing, the FBI's Anom server also swept up the assassins celebrating a successful hit.

"Now the Swede is gone," Kevin, one of the accomplices on the bridge, wrote.

"I am so happy bro," Abdul, another person involved in the planning of the assassination, wrote. "Hahahahaha."

In excruciating detail, it was all there. Potentially enough information to warn Sascha again or to stop the killers.

The Swedish police were locked out of intercepting these Anom communications. Just as they were with other encrypted phones criminals used in the country. Only this time, it was the FBI's own company that kept the Swedish police out.

Swedish authorities had seized one of the murderer's Anom phones the month before the killing. At the time, the police didn't even know it was an Anom phone. To them, it was just another device. Thanks to one of Anom's signature security features, they did not realize that the calculator icon hid a secret messaging app behind it. Nor did they know that the FBI already had the phone's crucial texts discussing the planned murder. In those, one member of the gang asked if Anom wiped like Sky.

Maybe if Anom hadn't existed, the murderers would have planned their act on another encrypted platform. At least some of those connected to the killing also chatted on Sky, for example. Or they might have used an ordinary telephone. In the end, those parallel universes were immaterial. The reality was that Sascha was now dead and his murderers planned it on the FBI's own chat app. At least there was evidence to perhaps prosecute the killers later.

As the plots for violence and other illegal activities continued to unfold on Anom, the FBI agents had an ever increasing number of jigsaw puzzles on their screens. Sometimes they only had some of the pieces, while others were in chats on encrypted platforms they did not control. Other times, because the messages came every few days, maybe there wasn't enough time to put the pieces they did have together. The FBI started to share more and more tips with foreign agencies, but it was still too late for Sascha.

When Anom expanded throughout Europe, the FBI found many of the messages were not just in Dutch but Swedish and German too. Much of this was thanks to Microsoft's continued attempts to make Anom the biggest phone company in the world. Confronted with the fact that a large slice of Anom's customers were international, and non-English-speaking, the FBI branched out. In September the FBI agents made a proposition to those countries just as Bobbitt had with the Dutch: they should use the intelligence harvested from Anom themselves. The FBI wanted to let these foreign agencies into Anom.

Blond-haired and blue-eyed Ted Esplund had a huge smile on his face. Inside the Swedish Police Authority headquarters in Stockholm, he was midway through a meeting with the local FBI legal attaché from the US embassy. Esplund and the attaché often had these meetings to update each other on what was happening on their side with ongoing investigations.

This meeting was different. Over coffee in the headquarters that looked more like a castle than a police station, the attaché had something to tell Esplund. First, though, Esplund needed to sign a bunch of paperwork. This was to ensure he understood the sensitivity of the conversation—what you can talk about with regard to the information, and what you need to keep to yourself or a select few others.

Now that you've signed the papers, I will tell you something, the attaché said. The FBI wasn't just intercepting messages from Anom. The FBI was secretly managing the encrypted phone company.

That's when Esplund's face erupted into a grin.

"The biggest problem for me at the moment, I just want to scream out to all my colleagues and everyone, 'Do you know what they have done?'" he later said. This sort of operation wouldn't be possible legally in Sweden, but the Americans had managed to do it. More astoundingly, the FBI had the criminals doing the work of selling the phones for them.

Esplund holding on to the secret wasn't actually a problem. He worked at Sweden's National Operations Department's intelligence unit. After a long time in the intelligence world, he knew when to keep his mouth shut. He looked forward to being able to tell his colleagues this incredible secret later.

He remembers it took just a few hours after his first meeting about Anom for his superiors to approve Sweden's involvement. Police in Sweden had already seen the incredible power of messages taken from underground chat platforms. After the Encrochat hack and subsequent arrests, the number of shootings and explosions in Sweden went down for the first time in years. Senior officials thought those messages had been a game changer in

combating serious and violent crime. Now the FBI was inviting them to a front row seat in the Anom operation. They did not hesitate.

The FBI provided Sweden and other European countries with detailed instructions on how to remotely access the Hola iBot surveillance system. The key point was not in how the system worked but in how the agencies could use it. The FBI asked them not to use the messages as part of their criminal investigations. The countries' prosecutors could not enter Anom texts as evidence in court to charge anybody. At least, not yet. Court meant discovery, and discovery meant revealing where the evidence came from. The FBI wanted to keep Anom going and its secret under wraps.

The FBI started a similar relationship with German authorities too. In a sign of how cautious the FBI was with this access, the agents did not even tell their German counterparts that the data came from Anom. The German Federal Criminal Police Office (BKA) figured that out themselves after they evaluated Hola iBot in October 2020.

All of this came too late for Sascha. The Swedish police gained access to Anom's messages two weeks after Sascha was shot on the bridge in Stockholm in mid-September. A short amount of time, but one that meant local authorities missed the chance to save him.

"This attempt to kill him—we could [have] stopped," Esplund said. The murder plot detailed in the Anom messages "was very clear."

Esplund's colleagues had thwarted gangland killings before; that was a key part of the job. Ideally, the police arrest the assassin before they act. There are other approaches too: if the police know the location of a planned hit, they can send patrol cars there. The blue flashing lights may scare off the would-be hitman and buy the police some more time. More time to find a way to reveal the shooter's identity.

Esplund didn't blame the FBI for not providing access to Anom's messages in time. If Swedish authorities had been able to read the messages in July, for example, maybe they would have found other missed crimes from June. Or access in May would reveal plots hatched in April. As well as the killers, Sascha was a victim of timing.

Swedish police came to call this event "The Bridge." A constant reminder of the stakes of Anom. The backdoor presented an incredible opportunity to surveil organized crime. But that opportunity carried

responsibility—the responsibility to act on that information if someone's life was in danger.

The murder pushed the Swedish police to never let a killing like this happen again.

"I will not sit and read on my laptop that someone is going to die between eight or ten this evening," Esplund said.

Microsoft was going to make the Swedish police's task much more difficult. The drug trafficker had a growing list of enemies who he believed owed him drug money. Just a month after Sascha's murder, Microsoft was preparing to go to war.

One target was Salah,[1] a former cafe owner in Stockholm who Microsoft believed owed him something like six to seven million Swedish krona ($800,000). Microsoft discussed kidnapping Salah to secure his debt and floated the idea of kidnapping Salah's son from soccer practice. Salah was only one soon-to-be victim of many: Copenhagen, Stockholm, and Holland were all said to be home to Microsoft's kidnapping targets.

This was about more than just the money. He said he wanted to strike fear into people. The kidnappings would be to build up and maintain a reputation. For that reason, Microsoft asked that the kidnapping be done in his own name. Victims would know it was Microsoft who had pulled them from their homes. Torture was on the table to send the message.

"Sadly we have to be violent too so people see that we go all the way," Microsoft wrote across Anom. "It has to be Mexico style on all of them," he added, referring to the brutal drug war violence in the country that he now wanted to bring into Europe.

Microsoft's campaign of fear would involve bombings too. Microsoft told underlings to stockpile as many hand grenades as they could. He wanted to throw the grenades at rivals' families and set off four explosions in Stockholm in one night. In Denmark he suggested shooting a target's father or brother in the legs, or blowing their door off.

Finally, Microsoft was prepared to murder. When one person in Spain owed Microsoft and his associate a debt, the associate took responsibility for sorting out the issue. He failed to do so, and the target walked away. Microsoft thought it was "shameful" his associate couldn't follow through with the hit. He wasn't hardcore enough, Microsoft complained.

So, Microsoft took matters into his own hands. He outsourced the hit to a trusted confidant, who in turn engaged with someone allied with FLG, a hyperviolent Swedish street gang. They said FLG had targeted three people recently. The gang could be bought by others, and Microsoft was willing to hire this street gang as his own personal mercenary force.

The confidant scouted the target's regular haunts such as bars and restaurants and a pizzeria. Microsoft and the confidant discussed every minute detail of the plan on Anom. Getaway cars, escape routes, what weapons to use, and how to give the hitmen Anom phones.

Microsoft ordered violence as casually as he did anything else. He said "let's brainstorm" when considering whether to kill or kidnap people as if he were in a normal corporate meeting. He punctuated his assassination plans with heart and thumbs-up emojis. Microsoft even asked if he could get a bulk discount from the hitmen if he ordered multiple murders at once.

For the moment, Microsoft didn't strike. He planned his list of targets, both in Sweden and abroad. But if someone didn't stop him soon, there would be an ever growing pile of bodies across Europe.

"All of Sweden will tremble my dear brother," he wrote to a co-conspirator on Anom. "I live for this."

Footnote

1 Author has changed this person's name.

Chapter 21

A Cottage Industry

There was something off about the neighbors. Lars[1] often saw the unusual group of men while he made coffee on his countertop brewer. His house in the Swedish countryside sat around one hundred feet away from that of the neighbors. As he peered through his floral curtains, Lars realized that the men who lived in the house used the front door to the property extremely rarely. Instead, they used a door to the basement whenever they came and went.

It wasn't just Lars who spotted strange things about the neighboring house and the people. Local residents noticed most of the windows of the house were open even when it was cold outside. The occupants would often dig and then cover a hole in the same spot in the yard again and again. And the men washed the car and van in the driveway inside and out much more frequently than they thought anyone else would do. One of the men in particular, Pawel Brzozowiec, cut the grass in the yard in such an erratic manner that neighbors thought he looked hysterical. For some reason, he always walked around in shorts and a T-shirt, even in Sweden's cold climate.

Brzozowiec seemed friendly enough. Clean-shaven, young, and with ears like radar dishes, Brzozowiec worked in a bakery late into the night. He sometimes gave bread he had taken from the bakery to the neighbors and offered them help with anything they might need. But some things were just not right.

This was Microsoft's latest project: an amphetamine lab hidden inside the basement of an idyllic cottage. While he pushed to expand Anom in

Europe in the second half of 2020, he also set up this lab in the heart of the countryside. The house was painted a modest beige and looked like a holiday home or a sleepy retirement spot. A few years ago, nearby residents noticed that workers started to renovate the house, but it still needed a lot of work. Inside masking tape still framed the windows, and the walls were half painted. The original idea of its owner—the father of one of the gang—was to later rent it out to fishermen. The village sat in between a dense forest and a Swedish lake.

The basement lab contained a cornucopia of dedicated and improvised equipment for cooking speed. In one corner was a machine for pressing the amphetamine into blocks. Nearby was a dough mixer that Brzozowiec likely had stolen from the bakery. Scoops, spoons, and forks caked with powder sat next to tubs of caffeine, solvents, and sulfuric acid. Flexible ductwork hung from the ceiling helped suck the poisonous air out from the basement. The smell of rotten fish wafted from some of the materials, and the two or three cooks wore protective masks as they worked. That smell was the vats of amphetamine oil that the cooks prepared to turn into amphetamine powder that could then be sold.

Microsoft's crew ordered the oil, which drivers then transported through Holland, Germany, and Poland to Sweden. The barrels of caffeine were originally manufactured in India and shipped from Poland. The cooks then took the mixture into a black tent-like structure that was set up in the corner of the basement. Inside were shelves where they stacked each glass tray of amphetamine mixture and left it to dry. As many as ninety trays could be in the tent at a time. Once ready, the cooks used the machine in the corner to press the powder into neat rectangular blocks and then vacuum-sealed them.

The lab was the evolution of Microsoft's drug empire. Rather than only handling the smuggling and distribution of narcotics, as he had with the speedboat full of cocaine, Microsoft now controlled the production side of the supply chain too.

Microsoft was associated with an alarming trend in Europe. Cops in Belgium, Germany, the Netherlands, Poland, and Sweden all found methamphetamine labs in their countries in 2020. The Czech Republic uncovered 160 methamphetamine-cooking operations across the same period. In 2019, authorities found and dismantled multiple cocaine laboratories in Europe. Then they found more the following year, including

in Spain. This was not just to fulfill the continent's own insatiable appetite for cocaine but also to export drugs to other parts of the world.

Those discoveries signaled a changing tide: Europe had become a larger producer of drugs. Europe was no longer just the end consumer.

Microsoft looked to be part of that Europe-to-overseas pipeline. He wanted to use his contacts to ship the amphetamine he was producing in Sweden all the way to Australia.

His men got to work.

Surviving on a diet of pizza and microwave soup, the cooks started by making a sizable fifty-seven kilograms of amphetamine in July. Less than two weeks later, they doubled their output. Microsoft hounded his cooks for photos of the drugs, even when they were busy trying to make the product in the first place. He wanted pictures to send to clients and kept pushing when he didn't get the exact photos he wanted, such as ones that showed the amphetamine in blocks. In August, one of the cooks fired back an Anom message saying they weren't going to take anything because they hadn't slept in three days. He was so tired he couldn't even think straight.

From the end of August and through September, the cooks doubled the amount of drugs they made again, and then some. Microsoft pushed one worker to produce more drugs before he planned to go on holiday that month. In total from the summer to the start of fall, the lab churned out an industrial 452 kg of amphetamine.

The one thing they didn't want to do was accidentally make "cotton," which is when clusters of pure caffeine form because the ingredients aren't mixed properly. A second issue was when the amphetamine turned a rancid yellow color, which is a chemical reaction due to a slow dry time. Their third batch had some quality issues, but generally the speed was of a solid standard.

The nearly half ton of drugs could bring in potentially over $1 million. Even after accounting for costs such as the amphetamine oil, which cost around $200,000, and paying the cooks, Microsoft stood to pull in a tidy profit from the lab. If the lab could keep running and expand as Microsoft wanted, he could make a killing.

Microsoft didn't control the amphetamine lab alone. He was part of a group of four people who called themselves the Firm. With fifty years in prison between them all, the Firm was no longer a hobby for its members. As the name suggested, they attempted to run themselves like a professional company. They told their lower-level employees that if they ever wanted to go on holiday, it had to be approved by "the board."

Tommy Bogebrink, known as Mr. Lansky or Zedd on Anom, was said to be a university-educated business lawyer and trained sea captain. He first met Microsoft in prison. Now out of jail for little more than a month, Bogebrink jumped straight back into criminality. He handled accounting and kept tabs on how much money each member had invested or withdrawn. He was especially tech savvy and sold drugs produced by the lab and others on the dark web. Here, websites that looked just like eBay or Amazon sold nearly every narcotic imaginable and shipped them in the mail. Dark web sellers sold drugs to both individual end users and wholesale buyers who were likely drug dealers themselves. The markets introduced new efficiency and security benefits: no need to meet other dealers face-to-face—including ones who might be violent—and buyers didn't need to know the right person to get what they wanted. They just logged on, found a well-reviewed product, and paid.

On these underground websites, the lab's amphetamine received a stellar average rating of 4.99 out of 5 from a hundred customers. Bogebrink sold wholesale quantities online too. The dark web wasn't just a place where more geeky dealers may find a way to sell some product. Serious drug trafficking organizations used it to supplement their ordinary income too.

Bogebrink was the measured counterbalance to Microsoft's erratic behavior. "You must not let him stress you," Bogebrink told one of the cooks in an Anom message. "He is not well."

The third member of the Firm was Alexander Jovanovic, who at times used the nickname Soko. He was an aging gangster with wavy silver hair who had known Microsoft and his family since Microsoft was a child. Jovanovic had retired earlier that year, but Microsoft convinced him to

come back to help with Anom. Now he was knee-deep in running the amphetamine lab too. The pair constantly bickered; Microsoft joked they were like a married couple.

The last member, MK, was something of an enigma. Bogebrink and Jovanovic did not know who this mysterious fourth investor even was. All they knew was that 50 percent of the Firm proceeds went to them and Microsoft.

Money from sales was then supposed to go back into the Firm's coffers so it could be invested in more projects. Some members brought in their own customers to then sell large quantities of amphetamine to. Bogebrink and Jovanovic had useful contacts for transportation and logistics for drugs in Sweden, and while Microsoft had similar, he was the one with global connections.

Each individual member may have owned an equal 25 percent of the Firm, but Microsoft saw it as his company. "This is not a democracy," he raged in one series of Anom messages to another member.

On Anom, the Firm had its own dedicated group chat for these four members. Below that main group chat were others, such as the "oil" chat, where those who had to organize the transport of amphetamine oil, spoke. Here and in direct messages Microsoft barked orders on how to run the amphetamine lab like an overbearing employer, including how to cook the drugs. At the bottom of the totem pole were a courier and getaway driver, the cooks themselves, and Jakub Walczak, a middle manager who oversaw the running of the meth lab despite Microsoft's constant nagging. Walczak's father owned the house, and Brzozowiec was his cousin. Microsoft made Walczak agree to work with him exclusively and no other criminal groups.

Microsoft and other members of the Firm then coordinated the sale of that amphetamine to wholesale buyers across Sweden. Drivers made drops in parking lots, near hospitals, and in quiet sections of the Swedish countryside. Microsoft remotely piloted these drop-offs. He acted as the relay point that hectically passed locations from the buyer to his own drivers and back again. Often he ordered customers to provide their car's model and license plate number, as well as an address. The customer's driver would leave the car parked there with the doors unlocked or the key hidden nearby. Microsoft's own couriers would then place the amphetamine in the car and leave. No one saw each other's faces. The drops didn't

always go smoothly, and some customers had to wait in the biting Swedish cold while Microsoft ferried information between the two parties. He also chatted with other criminals about exporting the amphetamine outside of Sweden.

Microsoft and his crew planned every element of the lab on their Anom phones. They used them for ordering the amphetamine oil, discussing techniques for producing higher quality product, and pinging back and forth to organize deliveries to customers. Microsoft's associates even sent photos of their vacations to one another across Anom. One photo included the sender lounging by a swimming pool.

The Firm didn't just use Anom phones—it became one of Microsoft's main vehicles for selling the devices. When Jovanovic relayed who needed new Anom devices, Microsoft sent the phones to them. And when Bobby was behind bars in Dubai, Microsoft took the opportunity to control more of the European market himself.

Around a month after Bobby was arrested and Microsoft pushed Anom more aggressively, people that Microsoft said were "the largest phone guys" were brought into Anom. Microsoft pitched it as an investment: if you were a high-ranking criminal, you could take these phones and then make money off the people underneath you in the criminal ladder.

Microsoft's resellers became more efficient. Jovanovic said he could get clients new Anom phones within half an hour. Their customers included Albanian criminals, whom Microsoft's associates also dealt drugs with. The Firm had its own drug operations and provided the technological backbone for others' as well.

Toward the fall, Microsoft traveled and took Anom with him on the road. He stayed in Madrid, and Anom phones started to appear in Spain.

Microsoft would later say he hired someone to be "the main man in Serbia," which slowly spread the phones farther east as well. Associates pushed into Denmark with Anom too, and Microsoft suggested he had shipped phones to Colombia. Colleagues told Microsoft to send the phones to Paris. One big break was a buyer who wanted to start with one hundred phones for contacts in Norway and Spain as well as Sweden. Potentially they thought this buyer would buy even more after that.

Sky was still the biggest player in Sweden and launched a ten-year anniversary promotion giving customers six months' worth of subscription

for the price of three. Ultimately, Sky became the de facto replacement for Encrochat in many places, not Anom. Microsoft would need something of a miracle to grab all of Sky's customers. But Sky still lost ground to Anom; the underdog nibbled at its ankles.

Microsoft's strategy was slowly but surely working. With Bobby mostly out of the way, Microsoft was now responsible for Anom becoming a recognized brand in Europe.

Microsoft wanted even more for his drug lab. In a message to the oil group chat, he sent a photo of a friend's lab that was able to produce three thousand liters a week. The large metallic contraption used in the cooking process was a silver cylinder with a small circular window in the side. It looked like a deep-sea diving vessel or a spaceship. "I will fill a swimming pool with oil for you," Microsoft dreamed in the message directed to Walczak.

Microsoft was well on his way to fulfilling this fantasy. The lab had reached the capacity to produce over a ton of amphetamine a month. On December 5, after the three large batches and as his cooks worked on a fourth, Microsoft was very happy with the lab's progress. He made plans to import more amphetamine oil every month so the lab ran like a factory. He even extended a compliment to Brzozowiec: he was impressed at the speed of the work. For the moment the group had only sold the drugs domestically. Microsoft told one of the group he had a line to Australia where the product could be sold for even more money—more money than they would know what to do with. He was now in contact with "the largest people in the world," he wrote. Police believe Microsoft's line to Australia was Ayik, the *Sydney Morning Herald* later reported. If the Firm could continue to make amphetamine, things would only get better.

"I'm starting to like you guys, maybe we can go on vacation sometime to a resort and drink beer and talk about the future," Microsoft wrote. He would pay for it all.

Microsoft sent those messages in the early morning. In just a day or so, his dreams would come to a sudden stop.

Footnote

1 Author has changed this person’s name.

Chapter 22

The Raid

There was to be no mention of Anom beyond the room, not even when the officers used the nearby toilets.

Inside a room belonging to the intelligence unit of the Swedish Police Authority's Stockholm headquarters, Esplund's team worked nearly nonstop across twelve or so computers. Members of the team put up dividers in the room, blocking anyone who walked in the adjoined corridor from peering inside. The team still shut the door and never mentioned the case outside of those walls. Here, in a mini version of the San Diego FBI's wiretap rooms, Swedish police secretly read the Firm's and other criminals' messages.

Through hours upon hours of reading Microsoft's messages, a case officer tasked with tracking the drug smuggler came to better understand what made Microsoft tick. One second he talked about a new plan to smuggle cocaine. Then, he threatened to kill his associates. Then, he flipped back again. A strange relationship started, with the officer developing something like a one-way friendship between himself and Microsoft.

The handful of agents didn't tell any of their other colleagues they somehow had data from Anom, even those from the wider intelligence unit that used the same bathrooms jutting from the corridor they shared. It was obvious to other teams that something significant was happening, though. People on Esplund's team were at their desks around the clock. The Anom work started while the team was still handling data from Encrochat. If anyone asked, Encrochat could be their cover for the nonstop activity.

There was then the additional secret that the Anom data had come from the FBI's secret management of the company. Only around ten people in the entire country knew the ultimate source.

Officers who were sent out into the field to act on intelligence got curious. The tips the intelligence unit fed to other parts of the agency were impressively detailed: a black BMW will drive to this parking lot at seven p.m.; the driver of a Volvo will then give this person a wad of cash in exchange for cocaine, for example. How was Esplund's unit getting this sort of granular insight on organized criminals' plans?

The criminals had managed to keep their own secrets too. Esplund and his colleagues had never heard of the Firm until Anom. Microsoft had whipped up an amphetamine lab right in the Swedish police's backyard.

The police decided to disrupt Microsoft's plans, not only to stop the flow of amphetamine but to apply some pressure to the Firm. If they could find the location of the lab and shut it down, Microsoft would owe other criminals money. Maybe then the Firm would get sloppy and make more incriminating mistakes. The intelligence unit could continue to monitor the group and gauge their reaction. Esplund wanted to rock the boat a bit.

It was time to squeeze Microsoft.

On a Friday in early December, Esplund called a contact who he knew could allocate staff to investigate the lab. Without saying how he knew, Esplund laid out in detail what the Firm was going to do: on Saturday, there is going to be an amphetamine deal in a specific parking lot. I think you should look into this, Esplund said.

The colleague was hesitant. We don't have the resources. Everyone is on other duties right now.

But Esplund persisted. "Please, do it for me, this time," he recalled saying.

The responsibility of investigating the drug lab ultimately fell onto Detective Inspector Andreas Börjesson. When Börjesson received the intelligence he did not know it was sourced from Anom—he only learned that later. But it was clear the information was good. The police didn't know where exactly the lab was. At the start of the month, Börjesson's team crept into action. They would follow the lab cooks and others to see where it led them.

Michal Glowka, with a massive jet-black beard and a bad back, downed a few drinks during his early morning flight from Warsaw to Nyköping, Sweden. To help keep up with Microsoft's insatiable demands for the lab to push out more amphetamine, the Firm hired Glowka from Poland to work as another cook.

With an Anom phone in his hands, Glowka provided the lab manager constant updates: I just got my plane ticket; now I'm about to step on the flight. He helpfully kept the manager abreast of his movements.

Those updates were helpful to another group of people. In the pickup lot of the airport, Swedish reconnaissance police lay in wait for the pair. They peered through cameras and snapped a photo of Glowka, wearing a blue jacket, and Walczak, who came to pick him up. After building on the intelligence from Anom, the police had followed the manager's car right there.

Once Glowka and Walczak met outside the airport, the pair got into a car and drove away. For the next several hours, Swedish scouts tailed the men both on foot and in vehicles. They watched as the manager went into a hardware store and bought the last gas mask filter in stock. At one point, an undercover police officer was just a few feet away from the manager while they both queued at the checkout. The store's camera filmed Walczak as he paid and walked out of the store.

The Swedish police also monitored other members of the lab team. The Firm had a vital drop to coordinate later that week—the one Esplund gave the tip about. The Firm had a new shipment of fifty liters of amphetamine oil arriving, enough to cook up another hundred kilograms of speed. A courier called Jens Lindberg would handle that. In his late fifties, Lindberg was reluctantly finishing a few last jobs for Microsoft before he planned to sever ties with him completely. He was sick of Microsoft's management style.

At the same time, the lab had produced a fresh load of at least sixty kilograms of amphetamine ready for customers. Brzozowiec the cook would transport that. The Firm needed to move both of these at the same

time, meaning the courier and cook would meet and hand these off to one another.

Brzozowiec arrived at the swap spot, a busy parking lot outside a shopping mall, at around three p.m. Dressed in a black jacket and beanie, Brzozowiec loaded a shopping cart with three boxes. These boxes contained the blocks of cooked amphetamine. He started to push the trolley across the car park while he held a phone in his hand to receive instructions.

A handful of Swedish police stealthily walked through the parking lot and updated each other on Brzozowiec's movements over their radios. First Brzozowiec wheeled the cart in one direction. Then he stopped for a short while and checked his phone. Then he performed a lap of the car park before coming back. Brzozowiec did not know where he was going. One police scout saw him look around nervously.

As Brzozowiec finally came toward Lindberg's car, Lindberg clicked his car key so the lights flashed. The trunk was unlocked. Brzozowiec loaded the three packages of amphetamine into the car. In return, he took out three white cans containing 50 liters of amphetamine oil. Brzozowiec loaded them onto his shopping cart and wheeled them across the parking lot back to his own vehicle. He then started the drive back to the lab. The swap was done, and the Swedish police saw every moment of it.

Lindberg, still nearby by his own vehicle, braced for the green light that he was clear to leave.

"Waiting for ok…," he wrote on Anom.

"Done!" Bogebrink, who remotely coordinated the swap, replied a few minutes later. "You can go." Lindberg jumped into the driver's seat and sped out of the car park. The police scouts followed in their own car.

They began to tail Lindberg. After a short drive on the highway, he took an exit and then pulled over. He stepped out of the car and went to urinate by the side of the road, leaving his phone on the dashboard.

The police pulled up behind Lindberg and got out of their vehicle. Lindberg immediately turned around from pissing in the ditch. When he saw the officers his face flushed with panic. The cops said they were going to search the car. Lindberg objected, but his body language said something else: he had given up. There was no way out of this.

When the police popped the trunk they found exactly what they were looking for: three white boxes containing what they suspected to be

narcotics.

Lindberg was supposed to make another drop that evening. He never showed up. Oblivious to Lindberg's arrest, the Firm texted him for updates but did not hear back. Maybe Lindberg had punctured a tire, or perhaps the battery on his Anom had died.

While one team of officers followed and busted Lindberg after the car park swap, another team had been consistently following Brzozowiec. At one point, Brzozowiec stopped somewhere to load more materials into his vehicle. As he moved sacks into the backseat, he momentarily looked straight in the vicinity of the police scouts. For a second, it seemed as if he stared directly at them. Brzozowiec's eyes locked with the center of the surveillance camera. Then, he turned away, oblivious to who was watching him.

After spying on them throughout the day, the Swedish police followed the gang of crooks to an innocent-looking cottage in the countryside. At six p.m., a police scout took a position in the forest overlooking the house. From the officer's perch hidden among the trees, they saw the gang's cars parked in the driveway. The air was quiet. The only hum of activity the officer saw was a person who briefly fiddled with one of the cars and then went back inside. The downstairs lights in the house turned on and beamed outward toward the forest.

The Swedish police had what they needed. The lab was probably inside this cute holiday home. They prepared to find out for sure.

At 7:30 p.m. Brzozowiec was upstairs watching a movie next to a half-eaten takeaway pizza when he heard a noise below him. The sleeping quarters of the drug lab were squalid, with beer cans, toilet rolls, and mattresses strewn across the floor. He headed downstairs to the ground floor. Despite it being December in Sweden, he wore shorts, a T-shirt, and flip flops because of the heat generated by the constant cooking of speed. He then started to descend the basement stairs.

Outside the house two SWAT teams of heavily armed Swedish police prepared to force their way into the building. Just twenty-two seconds after the teams pulled up to the house in their vehicles, they were ready at the doors. One team positioned outside one of the house's entrances. The second took point on another door that led directly to the basement. Simultaneously, the teams started the strike.

"Police!" one officer shouted as his colleague flung the basement door open. On ground level, a member of the other team smashed the front door's lock with a handheld battering ram.

Brzozowiec peeked around the corner just as one of the SWAT teams entered. He immediately spun around 180 degrees only to come face-to-face with the second team.

"What the fuck!" he screamed.

The officer at the front of the pack pulled Brzozowiec aside so the rest of the team could rush in. The officer then threw Brzozowiec to the ground. Two large thuds connected with Brzozowiec's body as the flashlights on the tips of the SWAT team's assault rifles rapidly strobed on and off. One member of the team panted heavily through his gas mask.

An officer then pushed deeper into the basement. As he entered, Glowka walked toward him, his black gloves caked in a powdery substance.

"Lie down! Down on the floor!" the officer shouted and pointed the laser dot on his pistol at Glowka.

Glowka immediately dropped to his knees, and then his stomach. The officer stepped over him, his laser still trained on Glowka's back, and shouted at him to put his hands behind his back.

Cautiously, the officer used the tips of his fingers to slowly open the door to the basement's second room. There it was: a mass of amphetamine production equipment, including a block press, tubes for ventilation hanging from the ceiling, and the tent-like structure for drying the product, as well as twenty kilograms of amphetamine.

The rest of the officers made sure the building was clear. They leaned around corners with their rifles pointed and checked upstairs. No one else was here.

Outside, the police kept away neighbors who had come to see what was happening with the house many of them had deemed suspicious. The whole raid was over in a matter of seconds.

When police grilled Glowka in an interrogation room a short time after his arrest, he claimed he had come to Sweden for a sightseeing trip. He was fascinated by nature and geography, he said. When asked why he was wearing gloves during the raid, Glowka said he had a cut on his right hand (that much was true), and that he didn't want it to sting while he washed clothes in the basement. Why, then, did he have gloves on both hands and not just his right one? Glowka said it was an old habit to wear gloves on both.

Glowka was lying through his teeth, but the police weren't being entirely truthful either. The interrogation, of course, was in a way a pantomime: the Swedish police already had all of the cooks' Anom messages, which showed in granular detail the amphetamine lab's operations.

The cooks remained unaware that Anom was to blame for their capture. When interrogators questioned Brzozowiec, the officers made no mention of the encrypted messaging app. Instead, they focused on the scene they found at the house, that of equipment used for the production of drugs. Media reports published in the days after the raid didn't include Anom at all.

The tension was that although Swedish police had dramatically raided a lab based on intelligence from Anom, they still, per the FBI's orders, had to keep the source of their information a secret. The Dutch, who launched their own interventions, had to do the same. How long the Swedish, or the Dutch, or the AFP, or the FBI could keep up this charade without criminals suspecting Anom was an open question.

Microsoft was furious. "How the hell did they find the lab???" he hammered into the Firm chat. The lab manager had watched the raid unfold

through motion-activated cameras installed in the house and then relayed the bad news to his bosses. He wasn't in the group chat because he didn't like Anom, telling Brzozowiec, "It's shit… I don't wont [*sic*] Anom in the kitchen." The cops completely cleaned house on the group. The lab was gone. Their cooks were arrested. And kilos of amphetamine and oil were seized. To add insult to injury, Microsoft didn't appreciate the dramatic manner in which the Swedish police cracked down on his drug lab. "They busted my team with helicopters and SWAT like we are terrorist," he complained.

The crackdown didn't make any sense. Only a few select people knew where the lab was. The Firm kept information from its workers on a need-to-know basis. The courier and the cooks who were arrested didn't even know much about each other; they couldn't have snitched.

The leading theory among the group members was that the police had somehow monitored the swap of amphetamine oil and product in the car park, and then followed Brzozowiec after the handover back to the lab. It wasn't clear how the police knew which car park to monitor, but Jovanovic and Bogebrink agreed there was no other explanation.

Microsoft focused on another part. Maybe the "TP," the transport, was compromised. In this case, that was the people who had delivered the amphetamine oil from elsewhere in Europe. The TP used Sky, as did another member of the organization. Maybe that was the source of the leak. From now on, Microsoft ordered, Sky would be strictly forbidden.

The supreme irony was that Microsoft had just sealed the Firm's fate of having more of its messages read. Sky wasn't the reason for the raid. Anom was. His suspicion was misplaced, and it would cost him even more headaches.

One reason the raid was so impactful on Microsoft was that, by his own admission, he always went all in. That could mean a massive payday. Or in the case of failure, he lost it all. Now he owed other people money for the loss. He said associates laughed at him when Microsoft explained everything was gone. Microsoft, just as Esplund and the Swedish police wanted, felt the squeeze.

A friend tried to assure Microsoft that maybe now was the time to slow down. Try a smaller job first, take your time. Microsoft was indignant; he wasn't going to do that. He thought the Firm should have grown the lab

even more. They had the capacity to churn out a massive amount of amphetamine, but their logistics structure of driving shipments to customers was too small. If they had expanded more aggressively, maybe they could have better weathered this raid.

In an Anom message, Microsoft made his intentions clear: “It’s not time for stopping now.”

He continued to aggressively push Anom without even taking a break. And Microsoft wasted no time throwing himself into one of his many other projects. Just two days after the lab raid, he told an associate he was buying cucumbers as part of a hash smuggling operation. Or perhaps he would purchase peppers, he hadn’t decided yet. A corrupt vegetable company in Spain was working with Microsoft, using shipments of their produce to hide drugs. After the shipment, Microsoft’s men could double-dip and then sell the food too. But they were out of their depth: Microsoft and an associate bickered over whether they needed to order normal-size or miniature cucumbers. The reason was that their vegetable buyer in Sweden might only be willing to take the smaller ones off their hands.

“Never sold green or legal merchandise before,” Microsoft texted as the pair figured out what vegetables would be best. He grew increasingly annoyed at the cucumber buyer’s request for only a certain type of product. “He is going to get a big cucumber in his ass soon,” Microsoft wrote.

Microsoft seemed to see the absurdity of a drug trafficker debating which cucumbers to import.

“We should open our own company, lots of vegetables every month for us 😂😂😂,” he wrote. But his erratic management style annoyed those underneath him. Behind his back, co-conspirators called Microsoft “the Fool.” He was about to ship drugs and vegetables into the country from Spain, while his associate hadn’t yet been able to find a safe location to drop the merchandise off. He told Microsoft he was doing it completely backward by ordering the shipment before he even had somewhere to unload it. Microsoft tried to offer the associate half of the money they made from selling off the surplus cucumbers as a sign of goodwill. It didn’t work. “I’m not a vegetable grocer and will not become one. If you want to become one, that’s up to you,” he texted back.

The white truck of vegetables and hash eventually arrived in Sweden in mid-December. Microsoft remotely masterminded the drop-offs from the keyboard of his Anom. He relayed a password for those on the ground to recognize each other—"Rolex"—and coordinated where each person was to meet.

There was still an issue: in the end, the truck was full of normal-size cucumbers. Microsoft said he ordered mini ones, but they didn't arrive. The buyer still wanted mini ones. Now the pair were stuck with an industrial quantity of cucumbers with no real idea of what to do with it. As he tried to find somewhere he could just dump the merchandise, Microsoft took his frustration out on the associate who was supposed to handle the ultimate sale of the vegetables.

"Thanks for nothing," he texted on Anom. "Then people wonder why they get shot."

Microsoft's lab was far from the only one carried in whispers across Anom. In another lab, this time in Greece, two men manually crushed pseudoephedrine pills to make a precursor for meth. They then poured the resulting liquid into containers normally used for olive oil and shipped those to Australia. Once the drugs arrived, a biker gang transformed the liquid into crystalized methamphetamine. Authorities believed with just a couple of the olive oil containers, the gang could easily make a million dollars.

One of the men never showed his face in Anom messages. He only showed his partner's. To the San Diego FBI agents scrolling through the man's messages, he remained a masked figure, always behind the Anom phone's camera and never in front.

Then, a fire started in the lab. A beaker violently exploded in the mysterious man's face. He took a photo to show the extent of his injuries. Finally, the FBI saw who they had been following.

"We were able to identify him because his meth blew up," Kalina later recalled.

When Kalina first started reading Anom's messages, the sort of labs he assumed were behind most meth production were makeshift setups in tiny apartments or warehouses. But as he continued to see more and more examples, his understanding of the scale of meth production changed. One lab he saw contained a seven-thousand-liter vessel. The group could produce that amount of meth every two to three days.

"And that's just one of these locations," Kalina said. Sweden, Greece, the Netherlands—Europe's transition into a meth and amphetamine hub was clearer than ever. Investigations that would ordinarily be started by police in each country individually were supercharged because the FBI was able to see them all at once. It would normally be considered a law enforcement success to monitor and shut down one sizable lab. But now the FBI detected at least fifty in one giant sweep. In parallel to organized crime's increased globalization, the FBI was taking its policing around the world.

Chapter 23

Metallic Maze

Near the base of a forest-covered mountain in Ecuador, an eighteen-wheeled truck drove south with browning grass on either side of the road. The truck looked like any of the countless others out on that day in October 2020. The burnt orange shipping container on the back of the truck contained cans of tuna. A very normal transport load for one of the world's largest tuna fishing industries. The driver was headed to Guayaquil, Ecuador's main port city.

The National Police of Ecuador received an alert: they should examine this specific container. While the truck was en route, police stopped the vehicle. A crowd of officers in black uniforms and high-vis vests surrounded the truck on the side of the road. Dogs trained in detecting narcotics set off further alarm bells. Something was up with this truck's cargo.

The police seized the truck and later unloaded its cargo in an antinarcotics warehouse. Boxes upon cardboard boxes, 181 in all. Neatly packed inside those were over eight thousand blue and green cans of what looked like tuna in vegetable oil. As officers yanked the ring-pull on top of some cans, they saw a yellow disc in each, perfectly shaped for the metal containers.

Those discs totaled to around 1,523 kilograms of cocaine. Over one and a half tons. A staggering haul.

The Ecuadorian police knew which truck to pick out that day because of Anom. Across their monitors in San Diego, FBI agents became acquainted with this particular drug cartel's plan. It funneled cocaine from Colombia

south to neighboring Ecuador, and then sent the drugs via container ship to Europe.

This sort of scale, with drug traffickers shipping thousands of kilos, took Muse from the FBI aback. Anom was in the hands of big-league drug smugglers now.

"Some of the key players in this investigation, they didn't speak in kilos, they didn't even speak hundreds of kilos, they only dealt in tons; they would only do business if they were talking about quantities in the tons, which to me was just astonishing," Muse recalled.

Anom ripped the veil off many more of those smuggling techniques. The FBI came to call one a "tile job." In one example, criminals owned an existing stone import and export business in Spain. The traffickers then ordered precursor chemicals for methamphetamine from India. Once the chemicals arrived in Spain, they had to smuggle them elsewhere. So the criminals put the precursors inside stone slabs. Half legitimate export, half drug trafficking operation, the slabs were broken up by accomplices at the target country once they arrived. Others hid drugs inside shipments of leather.

"If they could dream up a concealment method, no matter how far-fetched it was—concealing drug precursors in stone slabs of tile—they would do it because the investment was worth it," Muse said.

Anom's gaze into the fake tuna operation picked up a key detail: the name of the implicated tuna company. As the FBI read the messages, one of the agency's foreign partners was nervous. It did not want to let a shipment of cocaine this large even leave Ecuador. What if the cocaine slipped away? So, the decision was made to strike inside the country rather than when the cocaine reached its planned destination, which led to the truck seizure at the base of the mountain.

Many other shipments of cocaine-filled tuna cans had likely already arrived at their landing place. There, the cocaine was worth seventy million euros. The drop-off point: the port of Antwerp, Belgium.

Antwerp-Bruges was more a maze than a port. Overall, the metal labyrinth of shipping containers and warehouses stretched across 16,600 football fields' worth of space. Every day, new containers came in, stacked in towers, and others departed. Annually 290 million tons of maritime traffic moved through the port. A constantly shifting haystack in shape and contents.

Antwerp's port is deep inside Belgium, along the western Scheldt estuary. The main Scheldt River starts at the North Sea on the Netherlands coast before pushing into Belgium and then south into neighboring France. Antwerp being an inland port offered a much faster way into Europe than other locations.

The port was a beating heart of the Belgian economy. It provided direct and indirect work to 164,000 people and added value of €21 billion.

All of this benefited the drug traffickers that used Antwerp as an international smuggling hub. The port's sheer scale let traffickers' shipments blend in with the background noise of the port. The location meant their narcotics got on the road to other countries quicker. The legitimate Antwerp economy provided plenty of opportunity for traffickers to launder their cash through nearby restaurants or businesses.

Often Moroccan and Albanian groups unloaded the cocaine from the port. Most of the cocaine in Antwerp was probably the property of drug trafficking groups a short drive away in the Netherlands. These groups then sent the cocaine on to other European countries to be sold. Antwerp, along with nearby Rotterdam, became a cocaine gateway into Europe: according to one United Nations office, nearly a third of cocaine seized in 2022 in Latin American ports was to be shipped into Antwerp. Europe's insatiable appetite for coke provided sizable profits for traffickers.

Along with Antwerp's increased relevance in the drug trade came a tidal wave of violence through the region. Beyond the makeshift torture chamber police found during the Encrochat hack, Antwerp saw explosions, shootings, and kidnappings. Those threats even extended to the top of the political system.

Belgium's justice minister Vincent Van Quickenborne, a highly vocal enemy of the drug business, traveled to the UAE to sign a treaty designed to help arrest and extradite criminals, including drug lords, based there. Later upon his return, authorities uncovered an advanced plot to kidnap Van

Quickenborne. There were reports that, as part of the plot, police found a car packed with Kalashnikovs and bottles of gasoline near his house.

Authorities rushed Van Quickenborne and his family to a safe house. The minister was forced to cancel his public appearances. In a Zoom-style call with journalists, using a fake background to hide his location, Van Quickenborne said that Antwerp had entered a new phase of "narcoterrorism." "The criminal underworld is trying to destabilize society and fasten its grip on it. They are doing this by scaring members of the police and the judicial authorities, just because they feel we are chasing them," he said. Van Quickenborne was defiant and doubled down on his commitment to fight organized crime.

Cocaine brought a tangible shift in violence in Antwerp and Europe more broadly. One government report found that drug traffickers used violence more offensively. "The nature of the violence appears to have changed," the 2021 report read. "The booming cocaine market has entailed an increase in the occurrence of assassinations, shootings, bombings, arsons, kidnappings, torture and intimidation."

Just like Microsoft wanted, European criminals were going "Mexico style" on their targets and bringing that violence to the continent's towns and cities.

Not even the ongoing COVID-19 pandemic stopped Antwerp's transformation into Europe's cocaine springboard. When the coronavirus hit, many land trafficking routes became unusable. Established avenues like the movement of heroin from the Balkans to the European Union ground to a halt. The number of flights available from South America into Europe also fell dramatically. Street-level dealing dried up in some places. With nightclubs and bars closed, demand for drugs in Europe plummeted too. People simply couldn't get outside to party in the first place.

Through Anom, the FBI watched some drug smuggling operations fail due to COVID-19 interruptions. One crew planned a highly elaborate shipment of cocaine from Colombia up to Canada. They attempted to hide the cocaine inside barrels of petcoke, which can be used as a fertilizer. Twelve kilos of cocaine went in and soaked among the substance. Once delivered at the other end, a chemical extraction process pulled ten kilos of cocaine back out.

“They had it all ready to go,” Kalina later recalled. “And COVID hit.” When the borders closed, it shut this drug trafficking operation down. The drugs had nowhere to go.

The FBI was all ready to go too. Along with Canadian counterparts, the agents excitedly waited for that first shipment to come in. The FBI had pictures of the drugs, everything. But the shipment never arrived.

COVID-19 hit the encrypted phone business too in its own way. Before the pandemic, criminal organizations often had members spread across different phones. The money launderers were on one platform. The drug distributors were on another. The producers might be on a third network. That provided a security benefit: if one company turned out to be compromised by the police, the blast radius was limited to just that network. The FBI saw this firsthand; in some cases Anom only provided a peek into a certain part of a syndicate. It was as if the FBI were secretly in a room, listening to the criminals, but could only hear the conversations of those closest to them.

“It made it really difficult for us because we knew we could never get into those other devices the same way. So we were missing a big piece of the puzzle,” Kalina said.

COVID-19 made the criminals’ compartmentalization more difficult. Syndicates started to consolidate all of their operations onto one network. Some went to Sky. And some, fortunately for the FBI, put everyone on Anom. The FBI could now hear everyone in the room talking at once.

Smugglers, as they always did, adapted to the new reality—in this case the pandemic. As borders closed they tweaked their routes. They used different locations in Latin America to initially ship cocaine over to Europe. To ferry the drugs, they used fewer human couriers, since they might carry the disease and be blocked by travel restrictions. Drug lords pushed to get even more cocaine into Europe. They gambled on fewer shipments stuffed with more cocaine.

Despite some early setbacks to the flow of drugs, government monitoring agencies saw no real decline in supply at the wholesale level. The police still found massive, multiton shipments of narcotics as part of their normal operations. While other legal industries were in a complete crisis, the drug machine found ways to power through.

One mode of transportation faced less disruption than the others: maritime vessels, such as those pulling into Antwerp. Syndicates switched their cannabis and heroin shipments from land to sea. Smugglers focused on trafficking drugs hidden within legitimate supply chains that might still be operational. Like the flow of tuna from Ecuador. That was the context in which the FBI found itself tracking cans of cocaine destined for Antwerp.

Time and time again, Belgian police found Sky phones when they investigated criminal groups. As the Sky phones piled up in Antwerp, in 2018 police there quietly opened a file on Sky and the distributors who sold these phones to organized crime in the region. They set out to find whether Sky was a legitimate company or one that pandered to criminals, like Phantom Secure did. Even encrypted phones still piggybacked off of ordinary cell phone towers to transfer data, which gave some detail on their physical location. When the authorities saw a Sky phone connect to a tower, they then dispatched teams to that location or used CCTV footage to figure out who had the phone in their hands. Many of those users were indeed drug trafficking suspects.

Investigators then determined one of Sky's servers was in the same northern French city as Encrochat. That broadened the investigative team from just the Belgians to French authorities too. Peering into the server, investigators could see only the metadata of Sky customers—their usernames and group chat names. Investigators found eighteen thousand active Sky phones were in Belgium and the Netherlands. Then, unsurprisingly, around half of those were concentrated around Antwerp.

That investigation eventually grew into the plan to hack Sky that European authorities had told Young about. That plan ballooned further and roped in expertise from Dutch police. But when the tuna shipment came up, Sky continued to coat Antwerp in a thick drape of encryption. Anom let the FBI peek underneath some of that veil.

The FBI found something that shocked even the most seasoned investigators: a concentration of corruption. Specifically, one Anom user warned others to stay away from Sky because authorities could read metadata from the platform—exactly the capability the European investigators had obtained. This person had also known the police gained access to Encrochat messages at the time. But because this person was

sending the tips across Anom, in full view of the FBI, it appeared they didn't know the US was running that phone company.

"There's probably fifty people, as far as we know, in the world that knew about Sky and Encrochat," Young said. The messages indicated which country this person, whoever it was, was based in. The San Diego team tipped off that country: "You have a huge public corruption problem," Young recalled.

It turned out, the alleged leak years earlier to Phantom Secure's Ramos was just a small taste of purportedly how rotten some sections of the world's law enforcement agencies could be. The messages rarely included names, but mentions of corrupt judges and cops flowed across Anom.

"The amount of corruption we were seeing in this thing was astounding," Young said.

Antwerp was not immune to corruption either. Some of the port workers flipped and ushered drug shipments through for a fee.

Something like only 2 percent of Antwerp's containers were ever physically searched. Rummaging through the haystack with blind luck only got you so far. Anom trained a laser sight on that haystack. Where it pointed, police followed.

Around the same time Ecuadorian police seized the truck of cocaine hidden in tuna cans, US authorities sent a tip to police in Belgium. Another of the cartel's shipments arrived in Brussels. On Anom, the criminals shared specific information on which container housed the tuna cans. Local police found more than six hundred kilograms of cocaine inside. Anom had derailed the tuna cartel, again.

In 2015, authorities seized around fifteen tons of cocaine at Antwerp. Then thirty the following year. Then more than forty. Fifty tons in 2018. And 2019 saw just over sixty tons. Then in 2020, the year Anom helped find more Antwerp shipments, police found sixty-six tons of cocaine at Antwerp. Those ballooning seizures didn't mean fewer drugs were getting through. Sixty-six tons was only what the cops managed to find in 2020. What the nonstop growth really meant was that Antwerp was more and more popular as a trafficking hub. As seizures in Spain and Portugal went down, where much cocaine traditionally entered Europe, the amount went up in Belgium. The traffickers had moved ports. Later, Belgian officials said they needed more incinerators to handle the mountains of cocaine

marked for destruction. The Drug Enforcement Administration starkly compared Antwerp to Miami in the 1980s.

The truth was, these fake tuna shipments were probably a day-in, day-out business for the cartel. They knew what they were doing and had the connections to get the job done. The production line was not all that different from the tuna supply chain the criminals latched themselves to. Only the product was different. The very well concealed cans of cocaine likely did "get through, probably a hundred times," Kalina said. If it wasn't for Anom, "we would never know."

The snacks are always important during an operation. In San Diego, Young saw the FBI agents eating their stale Twizzlers and offered to buy the team some better things to munch on.

"Yeah, if you could make yourself useful, that would be great," Young remembered Cheviron joking back.

Cheviron was teasing, but the dig did hit at something true. With the legal architecture for Anom's international interception in place, there wasn't all that much for Young to do. The messages were rolling in—authorities were seizing shipments like those in Ecuador and Antwerp; European cops were squashing drug labs like Microsoft's.

So Young pivoted to shining a light on Anom's one remaining blind spot: the US. Finally, the FBI might be able to read the messages of organized criminals on their own turf. Whereas it took weeks or months to build the charts of names and photos in the wire room for international targets, the FBI could do the same in just days for suspected criminals in the US. After funding this operation, and helping countries around the world, maybe the FBI could get some domestic results. The FBI certainly wanted to monitor phones in the US, but the agents didn't have permission to do so.

The team estimated they could probably get up to four or five hundred phones into the country. Under US law, every time the FBI wanted to read messages from one of those phones, they would need to get a wiretap order for each individual device that popped up. That would be a mountain of

paperwork, but the team was prepared. They made boilerplate language so the wiretap application process would be quick. They were teaming up with the Los Angeles US Attorney's Office. The little brother had something to show its bigger sibling. Anom's secret would probably trickle out if the FBI did arrest anyone in the US based on Anom messages. This was due to requirements to show defendants the evidence gathered against them. The team would deal with that bridge when they came to it.

Just like Hanson, drug traffickers shipped cocaine from the US into Australia during Anom's rise. And Anom phones did land inside the US. The FBI created a block list of devices whose messages would not be processed into Hola iBot. Sometimes based on a device's GPS position, the block list was primarily created for Anom phones that sent messages from within the US. (The FBI also placed a restriction on phones inside Switzerland; a fear was potentially violating the country's strict privacy laws and getting arrested in Switzerland if anyone from the team ever went there. The FBI eventually lifted that restriction.)

Anom usernames on that block list hinted at criminality: ">Masin~Ak47<"; "Walter White," referring to the teacher turned methamphetamine producer in the crime series *Breaking Bad*; and even "Sinaloa 13." But the FBI was unable to peel back the curtain on those users and had to remain largely oblivious to what each said on Anom.

The team applied for their first authorization to monitor an Anom phone in the US. This could be the moment.

The request went to the Office of Enforcement Operations (OEO), the section that helps sign off on every federal wiretap in the country. Its office was just two blocks from the White House in Washington, DC. If OEO didn't play their part, you didn't get a wiretap.

Under OEO's own rules, Young believed it was supposed to make a decision within a few days. He was frustrated, then, that OEO sat on the Anom request for months.

"It was so obvious to me that they're just never going to approve it," Young said.

In Young's eyes, this was a wasted opportunity. Rather than focusing on the treadmill of border cases, San Diego was trying to do something new. With Anom, the FBI could perhaps finally get the Owen Hanson types who don't flash their criminality. The drug traffickers who fly under the radar.

The corrupt officials. Young wanted to monitor phones inside the US "for the same reason that we wanted to do [it] on the international side, which was getting people that never get got."

"They didn't want any blemishes, so they didn't want to do the kind of stuff that we wanted to do that we thought were actually impactful," Young said, characterizing the people who tried to stop Anom. Anom was "opposed to what the operating MO is for drug prosecutions in this country, which is just go after the easiest, lowest hanging fruit, which tend to be small amounts, minorities."

The team could have fought with its rivals day in, day out, and perhaps gotten approval for a handful of phones. But it wasn't worth it for such small pickings. Anom was about scale, and there was no political will to scale inside the US.

Young saw no way forward. After a thousand administrative paper cuts, he quit the Department of Justice at the end of summer 2020. He went on to join law firm Barnes & Thornburg, for more money than his government salary, in part to support his kids.

"They managed to kill the US part of it, and they did it through bureaucracy," Young said. The Department of Justice just wasn't the place for a disruptive startup.

Chapter 24

Hawala

Shortly after landing in Dubai, Abdullah Eizuldeen did what every self-respecting banker for the criminal underworld would do: bought a ticket for a dune buggy safari. Eizuldeen and his girlfriend zipped across the desert in the red and black, 2000 cc, custom-made vehicle. As his girlfriend wore a red helmet and left spiraling tire tracks in the dunes, Eizuldeen sat in the passenger seat and took photos. Eizuldeen, with a neat, short black beard, also went shopping for a $1,000 pair of sneakers from a Louis Vuitton store in the Fashion Avenue section of Dubai Mall. At night, the pair visited The Galliard, an extravagant restaurant in the heart of the metropolis. They also posed outside the massive Burj Khalifa skyscraper as fireworks cascaded along its sides. Eizuldeen and his girlfriend were clearly making the most of their New Year's Eve 2020 trip.

Dubai was a hotspot for money launderers who handled criminal proceeds. In one case, a gang operating in France took the cash from its cannabis business and physically shipped it to Belgium, where its members bought gold. After that, couriers working on the gang's behalf, who were often Belgian students, transported the gold to Dubai. Once in Dubai, the gold was made into jewelry and shipped to India to be sold in the country's domestic gold market. After that convoluted pipeline of drugs, cash, gold, and jewelry, bankers then split the now clean profits between the gang and the money launderers. The crew brought in a tidy 170 million euros annually.

Eizuldeen lived in Marbella, Spain, another city with a reputation as a hiding spot for the criminal elite. Earlier that year he traveled to Rome,

Italy, and Phuket, Thailand. As part of his business moving masses of gangsters' cash and all of that travel, Eizuldeen needed to be online as much as possible. He had been on Encrochat, and worked on Sky. When in the gym, he sometimes placed three phones on the floor next to one another so he could use them all at once. Now that he was in Dubai, Eizuldeen wanted to know if his new Anom device would work in the city, in case more work came up while there.

Microsoft, soon to be Eizuldeen's latest banking client, assured him it would.

"All my friends who need a changer I will send to you, you are the first on Anøm," Microsoft wrote to Eizuldeen. In exchange for pushing customers his way, Eizuldeen said he would fix the best prices for Microsoft he could.

Those prices were for Eizuldeen's professional service of moving money across the world. Drug traffickers couldn't just send the proceeds of drug sales in a normal bank transfer. At least not easily or without setting off alarms in the bank's compliance department. And smuggling cash across borders in briefcases took time and effort. That's where Eizuldeen's network of globally dispersed couriers and bundles of cash came in.

When Microsoft had money from sales of Anom phones or drugs, he sent Eizuldeen an address where the cash was. It mostly didn't matter which country; Eizuldeen's network covered the entirety of Europe, some of the Middle East, and Colombia, Brazil, Ecuador, and Mexico. Eizuldeen relayed that location to his money mules, and one of them turned up to take the money. One courier alternated between their black and white BMWs. Often cash pickups were inside homes, shops, and hotels.

To ensure the pickup went smoothly, Microsoft and Eizuldeen also agreed on a password. Sometimes this would be as simple as a word like "Paris" or "Madrid." Other times, the couriers used a "token." This token was the unique serial number on a bank note that the cash giver carried. They took a photo of this or typed it out. When the money mule arrived, they checked that the person they met held the bank note with that same unique serial. It was like a password but one that was impossible to guess and that, most of the time, changed after a deal was made. Much more secure. Microsoft's person holding the cash and Eizuldeen's picking it up

didn't even need to know each other's names. Just a flash of a bank note and they handed over the money.

Once the cash was picked up, Eizuldeen then updated Microsoft's balance in his "account," a spreadsheet Eizuldeen kept on his phone. When Microsoft then wanted to "withdraw" from that account, perhaps to pay co-conspirators in South America, the process went in reverse. Eizuldeen had a courier in the destination country make a cash drop to another location of Microsoft's choosing. Depending on the countries involved, Eizuldeen then took a cut between 4 and 9 percent.

Underground bankers stashed money in safe houses around the world, sometimes with reinforced doors and trip wires that triggered surveillance cameras. Couriers brought and removed cash to and from these locations as needed. If a courier decided to pocket more than they earned, they could expect to face serious consequences. No cash physically crossed borders, because money was already inside the destination country. It was Microsoft's balance that went up and down, just like an aboveboard bank. This meant Microsoft could have his wealth transferred to another country very quickly. Eizuldeen promised clients they would have the money wherever they wanted it in the world within twenty-four hours. And he often delivered on that promise.

The system also meant there wasn't a legitimate bank for the police to demand records from. No wire transfers to monitor for suspicious activity. No bank accounts to freeze. To anyone who didn't work with or for Eizuldeen, the transfers were completely invisible.

People like Eizuldeen played a crucial and unseen role in the drug trafficking industry. Out of the prying eyes of the heavily regulated banking system ordinary people used, this shadow economy let Microsoft and other criminals move funds internationally, unhindered and uninterrupted by law enforcement. Eizuldeen was an ATM, bank teller, and money launderer rolled into one. And he was just one of an ultimately untold number of these underground bankers. Known as hawala, this financial system started centuries ago before modern banking was invented. Now hawala, and its Chinese equivalent known as the fei ch'ien system, played a critical role in modern drug trafficking. If the police caught up with him, Eizuldeen had a colleague who he said worked "in the Arab countries" who could quickly take over the workload. The money wouldn't stop moving.

Eizuldeen offered something like the twenty-first-century version of hawala too: Bitcoin.

Bitcoin was also a system that ran in parallel to the mainstream banks. Rather than have a bank teller constantly track how much money was in a checking account, the Bitcoin network did this itself. Individuals and companies ran gargantuan computing rigs that verified which Bitcoin address had sent funds and where they ended up. In return and as incentive for providing the massive computing power necessary, the miners earned Bitcoins themselves. The end result was a self-sufficient financial network that didn't need to know, or necessarily care, what ordinary banks thought about it. Many touted Bitcoin as a private form of currency, resistant to surveillance.

Bitcoin made the borderless exchange of wealth even easier. All traffickers needed was a computer or mobile phone with a Bitcoin wallet app. Like hawala, there was no bank or credit card company to refuse the transaction. Bitcoin didn't need to wait for a courier in a black BMW either. Whenever Microsoft wanted, he could send funds of any size to someone else, directly.

Difficulty might come in cashing out those Bitcoin funds into fiat currency. Bitcoin exchanges like FTX and Binance, large companies that let customers buy and sell Bitcoin for cash, often asked for identification and closed suspicious accounts. Microsoft faced this problem before when an exchange shut down his account and those of around ten people associated with him.

That's where Eizuldeen helped again. Eizuldeen offered customers the ability to swap between cash and Bitcoin and back again if needed without one of these pesky exchanges. Eizuldeen was the exchange, and one that worked directly with criminals. He was the banker and tech support at once. Eizuldeen changed his Anom profile picture to that of a dollar and a Bitcoin sign and his username to "Bitcoin ATM/Money Transfer." If any Anom users wanted to swap one for the other, he was the guy to go to.

Cashing out from his banker in Bitcoin started to become Microsoft's preference. The system allowed him to deposit cash from various countries via Eizuldeen's couriers and then withdraw Bitcoin directly to a wallet stored on his own mobile phone. Ayik turned to Bitcoin as well. The

cryptocurrency's volatile value meant users may not want to hold on to it for too long, especially if they had people to pay. Eizuldeen offered a way to quickly cash that Bitcoin out.

Despite all its hype as an anonymous form of currency, in practice Bitcoin was very trackable. Following its creation in 2009, law enforcement agencies and private companies got more savvy at tracing the digital cash. In many cases it was trivial to follow a Bitcoin transaction from one wallet to another. Law enforcement, with their court orders and legal powers, then compelled Bitcoin exchanges to reveal who was behind a certain account. Bitcoin's promised cloaks of anonymity were more like a flimsy shower curtain, the subject's silhouette visible through it.

In some ways the lack of true anonymity didn't matter much to criminals like Microsoft. For them, Bitcoin was more about the fast and borderless transfer of wealth. Even if cops could see criminals sending Bitcoins to one another on the blockchain, so what? That information by itself didn't reveal where exactly they were hiding out. Yes, there was some legal danger incurred by having the transactions recorded, but those risks were more than offset by the convenience of moving money so efficiently.

South American cartels used Bitcoin for this intercontinental shipping of funds too. In a separate investigation the US Drug Enforcement Administration focused on a drug trafficking organization in Atlanta. According to a law enforcement intelligence summary, to start, the group received bulk drug shipments from Mexico. After selling the drugs, the group then logged in to a website called LocalBitcoins to purchase digital currency. LocalBitcoins was not an institutionalized Bitcoin exchange, one that handled the buying and selling of Bitcoin itself. It was more of a Craigslist-style site, where users could find individual people to buy Bitcoin from. Many of these people did not ask for identifying information from their customers.

After Bitcoins were purchased, the digital currency was sent to a broker in Colombia. They then exchanged it back into fiat currency and sent the cash on to Mexico. No need for duffel bags of cash across the US border, or wire transfers through banks. Authorities also found that the Sinaloa and Jalisco New Generation Cartels increasingly used Bitcoin to launder their money.

Borders meant very little to globalized drug traffickers who used this banking system. The smugglers' products may have been tied to a specific place by their physical nature—they could only sell drugs if they were able to get them into the hands of customers. But their finances faced far fewer limitations in the twenty-first-century world of cryptocurrency.

In one cash pickup, a Microsoft henchman wrote to Eizuldeen in an Anom message, "Brother tell him delete address so police don't get it where we meet today."

Deleting that information was, of course, futile. As soon as the underling hit send, Anom silently sent a copy to the authorities. By bringing Eizuldeen onto Anom, Microsoft had unknowingly opened a window into the hawala system and the traffickers' use of Bitcoin. The FBI peered in.

"We've got a lot of Bitcoin wallets, which is pretty exciting," Kalina from the FBI later recalled. Every Bitcoin address, bank account, cash pickup location. Anom saw it all. The FBI then sent those bank accounts to its international partners around the globe to investigate them further.

The FBI followed one group based in Europe that, like Eizuldeen's, did nothing but launder money. They sent runners who collected cash and brought it all back to a single safe house in the Netherlands. The couriers then stacked it in neat piles in a black soundproofed room, their equivalent of a bank vault. The stacks of cash, with the bundles sorted by different denominations of euros, covered a good chunk of the wall. After their collections, a member sent a photo of the haul from their Anom phone.

Conveniently for the FBI, the criminal superimposed the running total onto the photo itself. The authorities didn't have to figure out how much cash they were looking at. The launderers did the work for the FBI.

For some time, the FBI tracked this group and watched as the financial conveyor belt of the underground kept running. The FBI found the money laundering syndicate trafficked about forty to forty-five million euros a week. An incredible amount of dirty cash that moved freely. And, again, that was just one organization out of many.

“It was unbelievable,” Kalina said. “It was pretty crazy.”

With a banker now by his side, Microsoft had the means to push for bigger targets. Next on his list wasn’t a drug deal, though. It was someone else inside Anom.

Chapter 25

Black Boxes

On New Year's Eve 2020, while Eizuldeen partied in Dubai, Microsoft sat at a small office's boardroom table in Istanbul. A computer mouse, phones, and other equipment were strewn across the desk. On the wall at the head of the table hung a dazzling orange and white illuminated sign.

"Anom," the sign read. "Enforce Your Right to Privacy." Microsoft, in a jubilant mood, exchanged New Year's best wishes with a friend over WhatsApp.

"How do you like my office?" he texted.

"Luxurious!" the friend replied. "The president."

Since pushing Anom through Europe and elsewhere, Microsoft had moved long term to Istanbul. Before his departure, rivals threatened him. And in August 2020, police from the port of Antwerp—the port Microsoft said he had control over—briefly detained and then released him. Microsoft told associates he would never come back to Sweden.

Despite relocating, Microsoft was able to keep the cash flowing from his drug and Anom businesses thanks to his underground banker. He was safer in self-imposed exile and could plot Anom's expansion with Ayik there. The two were closer than ever, and Microsoft used this Istanbul office as his own.

Microsoft got up from his chair, walked toward the hum of the neon sign, and posed for a photo someone else in the office took. Wearing a light-blue button-down shirt and jeans, he gave a thumbs-up and smirk to the camera. He had reason to be happy: the coup had started.

This office was the physical manifestation of Ayik and Microsoft's takeover, an Anom-branded space above a cafe. Ayik launched the office, it seemed to other people inside Anom, to project power. Ayik wanted to show that he was the boss of Anom, at least in Europe. When Ayik first held a meeting with some phone sellers and Afgoo from his hotel's cafe a year earlier, he introduced himself as Anom's CEO. Since then he had willed that position into existence. Who else had the office space, conference table, and giant illuminated company sign if it wasn't the CEO?

Having an office in Turkey certainly did not make any practical sense. Sourcing phones in bulk to turn them into Anom devices was difficult in the country because all devices had to be registered with the government and a hefty fee paid. Instead, the office was a prop in Ayik's theatrical power play.

Ayik didn't even feel the need to tell Anom members about his idea to make an office. Some found out when Ayik sent sketches of his already planned neon sign. Other Anom workers, who saw the office in videos Ayik filmed, thought the lit-up logo was cringeworthy.

Microsoft showed off more Anom marketing material in messages to associates. One was a circular Anom sticker—the "Ø" in Anom—plastered to a laptop. Another was a laptop's desktop background. "Live by the Code," the desktop read underneath the Anom logo.

Sitting in the cafe below the office, Ayik often told Anom staffers that "the guys will be down soon with their laptops." Those guys were the new faces of Anom, what one worker dubbed "the Turkish Boys."

This ragtag gang was something of a family reunion for Ayik. The group included Erkan Yusef Dogan, Ayik's nephew, and Baris Tukel, said to be Ayik's cousin. Both men were Comanchero bikers, with Tukel a former sergeant-at-arms for the gang. Now he was deep into Anom and discussed a novel way of smuggling cocaine.

"There is 2kg inside french diplomatic sealed envelopes out of Bogotta [*sic*]," Tukel wrote to an associate on Anom earlier that year. Tukel didn't say in that message where he or his associates got the envelopes—be that a corrupt official or another way—but the envelopes were a trafficker's golden ticket. Ordinarily government officials used these pouches to transport sensitive documents from one embassy to another. Border officials were not legally allowed to search the contents of diplomatic packages, either physically or by X-ray. The smugglers believed their cocaine was

entirely safe from being discovered. The scheme worked: Tukel said in a follow-up Anom message that the packages landed in Brisbane, Australia. The group could smuggle two kilos of cocaine like this every week.

Tukel was close to Ayik and attended an extravagant meal in Turkey in 2015 celebrating Ayik's wife's birthday. Despite living in Turkey for years by now, Tukel still carried his Australian accent and mannerisms, which came out in voice memos sent across Anom.

Ayik, Microsoft, and Tukel often schemed in the Anom Istanbul office around the boardroom table. Sometimes those schemes focused on something that Ayik and Microsoft saw as a threat to their grip on Anom: a little black box.

Rows of mobile phones and an overgrown mess of cables lay on a brightly lit wooden desk in the Netherlands. The person tinkering with the phones, an Anom seller known as Wijzijn, reached out and tapped one of the black device's screens with his index finger, showing off his handiwork. The dozen-plus phones were each connected to their own white cable. Those strands then chaotically led to a four-and-a-half-inch black box.

Wijzijn turned around to a second identical setup behind him: another fifteen phones and cables connected to another black box sat on another desk. A bonsai tree sat at the top of the desk. These boxes were in fact miniature computers, and each had their own name: Bladerunner or Ripsaw, for example. It was the same tech that Afgoo had used earlier to jump on Encrochat's downfall. Now Wijzijn was trusted with his own boxes.

Finally Wijzijn turned to columns upon columns of stout cardboard containers to his right. Each box had an attached shipping label, soon ready to send across Europe or beyond.

This was inside Anom's new satellite factory in the Dutch city of Nijmegen, close to the German border. Previously, the electronics company in Hong Kong installed Anom's software onto phones. But after the fall of Encrochat, the company couldn't cope with the surging demand for Anom. Encrochat's death doubled Anom's user base. To keep up with the influx of

customers, Anom superiors provided Wijzijn with the black boxes to install Anom's software onto handsets himself. It was the same process the electronics company did in Hong Kong, or that Afgoo followed when listening to drum and bass music. Only now Anom had at least three factories rather than one.

By now, some three thousand people used Anom. Each with their own secrets, schemes, and syndicates. All of them unknowingly carrying an FBI informant in their pocket, a wiretapping operation of unbelievable scale.

The Anom app had an eclectic mix of profile photos users could personalize their account with—a who's who of iconic movie roles, politicians, and infamous gangsters. Nelson Mandela next to Pablo Escobar. Edward Snowden and David Hasselhoff. Snoop Dogg and *Scarface*'s Tony Montana. Those users also set custom display names, like someone might on their Instagram profile. Dozens upon dozens of criminals used "James Bond."

With the FBI's continued direction of what updates should be pushed to Anom, these thousands of users could quote one another, in a similar way to how people quote-tweeted each other on Twitter. They could also forward messages from one person to another, like how posts on WhatsApp sometimes went viral. Anom launched the ability to do @ mentions too.

"Imagine on Instagram and Twitter, you can mention a friend or coworker if you want to show them an interesting article, or something funny, or whatever," Muse said. Anom users tagged their cohorts to bring them into different criminal jobs. Anom was no longer a simple messaging application. Anom became a social media network for drug traffickers. Anom was organized crime's Facebook, conveniently for the FBI, mapping each gangster's social and professional connections.

And back in Europe, Wijzijn's black boxes continued to accelerate that growth. At one point, Wijzijn expanded beyond the phone shop he worked in and flashed the devices in a warehouse.

Wijzijn had pushed for access to the boxes. That would take some of the pressure off of the electronics company in Hong Kong. And the export duty cost of sending phones from Hong Kong to Europe added up. The boxes bypassed the need to pay customs a large fee because the devices were created in Europe. Wijzijn instead downloaded the Anom software from the internet and installed it himself. The black boxes were springboards that

sellers could jump from into more markets. Anom's idea was to have one or two of the boxes per region and only with trusted people.

The FBI worried about what this meant for Anom. The Hong Kong electronics company was a bottleneck that controlled the flow of Anom phones. That let the FBI grow Anom slowly, bit by bit. The boxes did away with that restriction. On one side, they made Anom much more efficient, better able to capitalize on the vacuum left by Encrochat. By the same token, the boxes were a powerful weapon that gave much more latitude to whoever wielded them. They got to decide who received Anom phones. It was not unthinkable that the FBI might lose control of Anom's fairly tight distribution. At the time, some new distributors had to apply through the password-locked website. The black boxes threatened to sidestep that protection.

For the moment that risk was theoretical. Wijzijn was the first, and for a while only, person outside of Hong Kong to receive any black boxes who wasn't also working for the FBI. Wijzijn continued his side of the encrypted phone business, with his own staff and customers as normal.

Anom also became more agile with the launch of its own portal. This was the dedicated reseller website Bobby demonstrated to Ayik in his hotel a year or so earlier. At the time, Bobby said if you wanted to scale the company, you needed a portal. Anom now had its own.

Again, like the black boxes, this took more control away from Afgoo and put it in the hands of individual sellers. For much of Anom's life, phone sellers woke up at all hours of the morning to be online at the same time as Afgoo. The Anom creator then activated the new customers' phones for them. With the portal, that capability transferred to the sellers themselves. They renewed customer subscriptions and signed up new clients. The resellers could bring on whomever they wanted.

In the pursuit of growth, Anom's optimizations opened up the company, and the FBI, to more risk. Risk in that Anom would swim in so much data a vital message might go unseen.

For Ayik and Microsoft back in the Istanbul office, Wijzijn and his black boxes were an issue that needed resolution. Wijzijn could flash phones whenever he wanted. Even though Wijzijn was on Ayik's European turf, Wijzijn was free to do his own thing. To Ayik and especially Microsoft, Wijzijn was a threat.

Ayik and Microsoft's perception was wrong—the pair were higher up the totem pole than Wijzijn—but that didn't matter. If the pair could get ahold of the boxes, the devices would then provide them an opportunity. Ayik may not have been able to buy a chunk of Anom as he wanted, but he and his lieutenant Microsoft could take it over from within.

"As soon as we have full control over Anom, you see," Microsoft told an associate in the winter of 2020.

What started was a long-running conflict between Microsoft and Wijzijn. Anom already had to compete with other encrypted phone companies. Now its sellers fought among themselves.

In Sweden, Microsoft ordered one of his resellers to remove Wijzijn as a contact from any remaining phones he had. That way, customers would be unable to go to Wijzijn for support and would only be able to go to Microsoft's sellers. Microsoft also told his banker Eizuldeen to cease contact. Microsoft was cutting Wijzijn out.

Wijzijn didn't remain passive. He had one of his own staff contact Microsoft's sellers in Sweden. Would they want to jump ship over to Wijzijn's team?

Over time both Microsoft and Wijzijn complained to Anom headquarters about one another. The company's other staff played mediator, and sometimes therapist, to both sides. Anom workers privately asked Ayik, Can you get Microsoft to calm the fuck down? Stop hassling Wijzijn; he is a huge mover of phones, especially in Germany.

Ayik and Microsoft escalated. They wanted the boxes. So Microsoft took the matter into his own hands. He sent someone to physically repossess the black boxes from Wijzijn, and then took other sellers' black boxes too. Originally the black boxes were a means for Anom to ease its supply chain issues. For Microsoft, they became a tool for exerting control. With Ayik's backing, Microsoft decided which sellers got a black box. The pair brought in more of their own people to buttress their ranks. Many of these distributors were not properly trained in using the boxes. Anom

phones went out to customers not programmed properly or incorrectly labeled.

But the takeover was a success. Territory that was originally for Wijzijn was now the property of Microsoft, and he determined who served which market. Microsoft now directed his banker to take cash from Wijzijn. Anom sales in Liverpool, UK, and Marbella and Barcelona in Spain filtered through Eizuldeen's laundromat.

Demonstrating his superiority over Anom's European operations, Microsoft took a photo of the portal that listed all of his resellers. In alternating lines of black and gray like a spreadsheet, the photo showed agents with Finnish, German, Italian, and the European Union flags in their usernames. Paris and Barcelona were also under his reign. At the top of that list, in all capital letters, was "WIJZIJN." Microsoft had won.

He wrote to an associate, "Wijzijn works for me."

Act IV

Chapter 26

Juggernaut

In February 2021, the impossible finally happened. A message flashed across the screens of dozens of police officers in Belgium, the Netherlands, and France. Investigators had managed to access millions of Sky's seventy thousand active users' daily messages in near real-time. For the next three weeks, they built cases around suspects in Antwerp and beyond. The authorities intervened when they spotted threats to life in the messages. The texts showed traffickers juggling several narcotics shipments through Antwerp at once—tons of cocaine, millions of euros every week, and corruption at multiple levels of society. The police identified clues to seize fourteen tons of cocaine.

On March 9, the agencies were ready to make themselves known. Early in the morning in Belgium, dozens of criminals were awoken by the country's special forces and federal police. They arrested forty-eight suspected Sky users. In the Netherlands, Dutch police simultaneously kicked down doors and arrested thirty people. In the lead-up to that day, Dutch police also quietly arrested an additional forty suspects. That was a relatively small number of arrests, but the real value was in the massive bank of Sky messages investigators could now mine for future arrests. As well as the three-week period of live messages, the team managed to decrypt hundreds of millions of historical Sky messages too. These raids were really just the start of the work on Sky.

Shortly after nine a.m., Microsoft texted an associate: "Brother. Think Sky is down." Something was wrong. Sky had sent a message to its users saying it was facing some technical difficulties, but now users faced error

messages when trying to log on. Soon, local journalists turned whispers into reportable facts: authorities had hacked Sky. Law enforcement had breached an encrypted phone service, again, and hoovered up users' messages.

The secret leaked out early to some. In late February, a member of one criminal gang said they ditched Sky for another provider. Sky was not "safe" anymore because police were intercepting Sky messages, they told an associate.

Sky was so confident in its product security that the company offered a multimillion-dollar bounty to anyone who managed to break into its communications. At a press conference announcing the hack, Belgian federal prosecutor Frédéric Van Leeuw said, "We will send… the account number of the federal police."

Despite the massive dent to its security-focused image, Sky, and its CEO Eap, clung on. Eap claimed his service was not a hotbed for criminals. Instead, he said Sky existed to protect people from criminal hackers and data breaches.

What few knew was that the hack of Sky was part of the much grander master plan to force criminals over to Anom. The operation wasn't so much about the arrests that day. It was what might happen next.

The European police had fulfilled their part of the plan by hacking Sky. Now, the American authorities took their first step in shuttering the app.

On Friday, March 12, a few days after the Europeans announced the hack, Eap received an unusual message on the encrypted chat app Signal. It was a journalist asking for comment on the newly unsealed indictment against him and whether Sky was still up and running.

"Sorry what indictment?" Eap replied. The journalist sent a link to a US Department of Justice press release. Its title: "Sky Global Executive and Associate Indicted for Providing Encrypted Communication Devices to Help International Drug Traffickers Avoid Law Enforcement." The court document accused Eap of violating the RICO Act, just like Ramos. The file San Diego prosecutors opened on Sky years earlier had borne fruit.

Eap went silent. He did not respond to the journalist, at least not right away.

After ruminating over the weekend, Eap provided a statement: "the unfounded allegations of involvement in criminal activity by me and our company are entirely false." He added, "in the coming days, my efforts will

be focused on clearing my name of these allegations," Eap said. He also said the indictment "is an example of the police and the government trying to vilify anyone who takes a stance against unwarranted surveillance. It seems that it is simply not enough that you have not done anything illegal."

"There is no question that I have been targeted, as Sky ECC has been targeted, only because we build tools to protect the fundamental right to privacy," he said, referring to another name associated with Sky.

Eap might have tried to save his name, but he couldn't save his phone network. The day after Eap's statement was published, the US seized Sky's web domains. These were Sky critical infrastructure, used for routing customer messages. As they had with Phantom Secure, the US authorities posted a message to Eap and Sky's customers. "THIS WEBSITE HAS BEEN SEIZED," it read, along with the coat of arms for the FBI and a handful of other agencies. BlackBerry then disconnected Sky's UEM services, the tool it used to push updates to Sky phones.

If the European hack shattered criminals' trust in Sky, the US seizure of its infrastructure finished the company for good. "We are going to need to shut down the service to be extra precautionary," a message from Eap to his remaining users read. "We will shut the services down in 2 hours to allow you to find alternative communications."

With little more than a good luck and goodbye to its customers, the juggernaut was dead.

Now, the most critical moment of the master plan. With Sky no more, would Anom become the new phone of choice? Would criminals flock to the FBI's own startup?

"We knew that they need to transition to something else that is available, that has a good name, that has a good reputation, and is basically a good platform," Andy Kraag, head of the National Criminal Investigations Division at Politie, the Dutch police, said. Kraag called it the "waterbed effect." When pressure was pushed onto Sky, "those criminals would spill out. They would have to find another encrypted platform to communicate on. And we just made that part of the master plan." Kraag saw Anom as the Rolls Royce of encrypted phones. It had all the features an international drug trafficker would want. Some of those Sky users would, hopefully, now go to Anom to be monitored even more. The shutdown was a purposeful,

anticompetitive practice: unceremoniously kill the rival, and further monopolize the marketplace.

"So when we do our Action Day on Sky, that's when you need to be ready, because most of them will transition to Anom," Kraag said, explaining what the FBI needed to do.

Before Young left the Department of Justice, he told one senior official how to prepare in the event that the Europeans did manage to hack Sky. "Buy ten thousand phones," Young recalled saying. "Because as soon as Sky goes down, you're gonna need ten thousand phones." In San Diego the FBI lay in wait, ready to absorb Sky's exiles into Anom and start hoovering up their texts too.

Sure enough, the earthquake of Sky's closure created a tsunami. A tidal wave of users who needed a new encrypted phone headed straight in Anom's direction.

Anom's management group chats bustled with activity. Anom already knew it would be an intense period after what happened with Encrochat. But nothing could have quite prepared them for the complete onslaught of new customers. Sky's dismantlement was the most transformative moment for Anom since its creation. This was the big rush.

For the next few weeks Anom went into overdrive. Staff worked sixteen-hour days, seven days a week, nonstop. Customer support was flooded with new signups, so much so that they hired more people to cope with the fresh demand. It was difficult to train new people in time; the customers just kept coming.

Many of those new clients were from countries that Anom had never seen before, or ones that up until this point only made a small slice of the user base. While Anom's expansion started in Australia and Europe, it then spread through South America, North America, and Asia. Border officials made importation into mainland China especially difficult. Customs seized heaps of Anom phones, but the company kept pushing.

Anom's backend engineers upgraded the phone network's infrastructure to handle the exponential growth in traffic. Conversations were kept to a staccato rhythm to save time: Order this many phones. Okay. You speak to this person yet? On it. There was no space for pleasantries.

"Chaos, complete chaos," an Anom worker later recalled. "Not much sleeping happened."

Christof,[1] an encrypted phone seller who worked under Wijzijn, had recently left Sky when he found a security vulnerability in the phone's software, which he says the company refused to fix. Now a vendor for Anom with his rich Rolodex of customers, his superiors gave him an order: "Push, push, push." From his oceanside, four-story penthouse apartment and nearby office in Europe, Christof got to work. On his laptop he usually kept in the bedroom, Christof signed up new customers through Anom's portal. "Get as many customers as I can, as fast as I can," Christof recalled the strategy being, to capitalize on Sky's death.

This was the opportunity of a lifetime for an encrypted phone seller. No rival as big as Sky had ever fallen. Christof and others had a real shot at making Anom the number one encrypted phone company in the world.

Higher-ups told Christof to sell phones at a steep discount, sometimes as little as 750 euros for a six-month subscription. That was an incredible price for an encrypted phone. If you were a former Sky customer, it would be nonsensical to not take the deal.

And the customers came. Anom distributors bought Google Pixel phones to flash in such large quantities that it became hard to find more to buy. Stock levels lowered to the point where Anom sold phones without ArcaneOS installed on them, and instead just the Anom app. There wasn't time to source the necessary, higher-grade smartphones that could handle the custom operating system. Anom superiors couldn't help Christof source phones so he tapped his own contacts. It was every seller for themselves.

That wouldn't be enough; Anom simply needed more phones. The company's invisible government investors decided to intervene.

Shortly after the Sky shutdown, Bobbitt the FBI legal attaché and a handful of colleagues drove across an airfield in the Netherlands to meet an FBI Gulfstream jet that had just flown in from Washington, DC. Inside the plane was a delivery: eight heavy duffel bags filled with around a thousand

Google Pixel phones. Bobbitt, his FBI partner, and his Dutch armed escorts wanted a quick offload with few, if any, questions from customs. Late in the day while it was still light, they unloaded the bags from the jet, put them into their truck, and drove off.

The FBI had heard the chatter among Anom's sellers that it was hard to source handsets. If the stock issue were not sorted, Anom's expansion, and the FBI's surveillance of criminals, would stall. But the solution wasn't as simple as placing an order; for one thing the lithium batteries in the phones could pose a threat to a commercial airliner. The agency decided to step in; Cheviron secretly bought the thousand phones to seed the supply and had them flown on the FBI jet.

By midnight the next day, the Dutch police arranged for the devices to be covertly left at a dead drop for Anom's local distributors. Anom's sellers got the phones they needed, without ever knowing the FBI had helped them.

Stock replenished, Anom's distributors continued to capitalize on Sky's downfall. Christof shipped Anom phones to Peru and Colombia. To avoid searches by border officials, he didn't mark the boxes as containing encrypted phones. Instead, on the invoice he had to provide the shipping companies, he wrote they contained "refurbished/used" phones. Ironically the phones sold really quickly in Lithuania, the very country facilitating Anom's worldwide surveillance. Christof and a reseller underneath him swept up just under five hundred customers in all. His customers liked the small details—the ability to edit photos and send voice memos, and Anom's ease of use.

South America and Europe were all good, but word trickled down from Anom's top brass, to Wijzijn, and finally Christof about a new target. They wanted to penetrate what might be one of the most infamous criminal markets on the planet: Russia.

Corruption was more than just a business in Russia, it was an institution. Organized crime was allowed to prosper at every level of the state. The country's oligarchs and their minions were exactly the sort of people who could have used a robust, encrypted platform to plot their crimes on.

Christof wanted to move into the Russian market when he sold devices for Sky. But he didn't receive enough support from the company to do so.

Anom was another chance. By his calculations, he expected to find between four and six thousand subscribers in Russia and neighboring Ukraine.

Christof had laid the groundwork for the Russia push before Sky fell. After that, the project took on a new urgency. Christof's bosses bombarded him with questions on the Russia expansion. Why aren't you moving fast enough? they asked. This business, Christof explained, was built on trust. Clients trusted Christof with sensitive information. That included what the customer looked like if they ever met in person. Or details of their business if clients ever disclosed them. Most of all, customers were trusting Christof with the security of their messages. Christof had a reputation in the encrypted phone world as a consummate professional. But for new customers this would take time. Trust doesn't build overnight.

It also wasn't as simple as sending phones to an address in Russia. Similar to Dubai, Russia had a history of heavily monitoring encrypted means of communication in the country. The country had legislation that compelled communications providers, including internet and web companies, to install lawful intercept equipment on behalf of the FSB, Russia's notorious domestic intelligence service formerly known as the KGB. This was so the agency was not locked out of messages sent by a particular company, app, or network, and it could read the content of people's communications if it wanted to. Telegram, a hyper-popular app that offered partial end-to-end encryption capability, moved its offices to Dubai, out of the immediate reach of the Russian authorities.

Anom had to sell its phones in Russia unofficially and subtly, so as to not gain the attention of local agencies that may not appreciate a chat platform suddenly offering a service their intelligence officers did not have access to. Christof would have to sell Anom even more stealthily than he did in other countries. Border officials would seize the shipment if they realized it contained encrypted phones. That sort of merchandise was valuable. That was "how it always works in Russia," Christof said. For Ukraine, he discussed the need to possibly bribe border officials to let the Anom phones through.

Christof tapped a contact he had in Russia and smuggled phones into the country via Estonia. They discussed a plan in which customers would buy Bitcoin in Moscow and then use that to pay for the phones. To start, he sent around fifty phones to Russia—some "big players" wanted to test Anom

out. Anom headquarters shipped SIM cards to Moscow to get their new customers online.

A while later, a tell-tale sign showed the phones had arrived. Anom support received inquiries from new customers. The messages were in Russian.

That initial Russian interest turned into a huge emerging presence in the country. With a clear demand from customers in Russia, Anom scrambled to make it official. In April, the month after Sky's downfall, Anom pushed an update that included a Russian language addition to the phones. That same update also included Albanian and Portuguese. Adding languages cost money, so Anom only did it when there was a serious appetite from speakers.

This was a moment that Silicon Valley CEOs sometimes described as "hockey stick growth," in which the number of users suddenly streamed upward, unabating, so that the resulting growth chart looked like a hockey stick. Whereas Encrochat's downfall had doubled Anom's user base, the downfall of Sky tripled it to roughly nine thousand.

Anom was comparable in size to Phantom Secure, the company the FBI originally emulated. The FBI was even better at this than some of the real industry players, and Anom was now a top player in the overall market.

"It was crazy. It was like we had started all over again, with new organizations, new information, new countries," Kalina said.

Anom also took a large bite out of Ciphr, Australia's dominant encrypted phone company. Thanks to Ayik's constant pushing of Anom, and news of an unrelated case in which police infiltrated Ciphr handsets to break up a drug deal worth tens of millions on the street, even more criminals flocked to Anom. If you wanted to keep doing business with the Comancheros, you needed to be on one of their phone platforms. That platform was now Anom.

The increased share of the underground tech industry allegedly led to massive profits for some of Anom's sellers. The US government believed some distributors made millions of dollars from the business, a business that ironically the FBI secretly funded.

The black boxes that installed the Anom software came into their own in the post-Sky rush. With these satellite hubs, Anom sellers quickly fulfilled orders from new customers. After Europe and South America, Anom

pushed farther into Southeast Asia: Thailand, Malaysia, Vietnam, Cambodia. A box in Thailand allowed sellers to flash phones without the need to smuggle them past border cops. Thai customs kept seizing the phones or charging a high duty rate.

One of Ayik's distributors urgently needed a box. Anom found a quick solution, but one that would have serious unintended consequences: the company showed Wijzijn how to "clone" the machines. The system was modified in such a way as to make copying the computer harder. Shown how to circumvent that, Wijzijn now didn't need to wait for Anom to assemble and ship a new black box. He could make one with his own computer equipment. It worked, and the distributor got the box they needed to keep expanding Anom.

But the genie was out of the bottle. The technique for cloning the boxes filtered up the chain to Ayik. Ayik now made black boxes of his own. The means of production were now entirely out of the hands of Afgoo, the distributors that Anom originally assigned black boxes to, and even the FBI. Ayik called the shots now. His team, including Microsoft, made Anom phones as they pleased. Anom management paid for a satellite office just outside Stockholm, and the Firm's Bogebrink got his own box to flash phones. In all, around ten black boxes popped up around the world.

The San Diego agents constantly assessed the black box situation and saw the tech spread around the world. In a way, the San Diego FBI knew this day would come. Because the agents wanted to copy real encrypted phone companies, they knew they had to give some power to Anom's distributors. The FBI always wanted Anom's growth to be organic, but with constraints: the FBI had fail-safes if a phone appeared in a part of the world it didn't want to surveil; at the start, Afgoo had to activate the phones himself. The FBI was already concerned that the existence of these boxes meant that Afgoo was ceding distribution of the phones.

Now some of the guardrails were blown off entirely. Anom superiors lost control of how Anom was sold in Europe, and Ayik finally had the power he wanted. Anom grew out of its test tube and took on a life of its own.

Footnote

1 Author has changed this person’s name.

Chapter 27

Squeezed

Microsoft was feeling the squeeze in the Istanbul office. Seated at the conference table with the Anom sign in front of him in late March 2021, he scribbled acronyms and numbers onto a paper notepad. His left-handed scrawls were messy, but the status of his drug trafficking was very, very clear: money was not good.

"Searching for projects, counting loses 😩," he texted on Anom along with a photo of his notes.

After the raid on his amphetamine lab in December, Microsoft had soldiered on with other ventures. The hash hidden among the vegetables totaled to a respectable hundred kilograms. Soon after that, things started to go wrong again. Several of Microsoft's drug operations went under as police jumped on more of his shipments. To Microsoft and members of his crew, the seizures may have been down to bad luck or poor planning. But the constant through line was really Anom. Law enforcement agencies continued to apply pressure to Microsoft, all the while he couldn't tell where exactly the pressure came from.

First, one of Microsoft's crews tried to smuggle amphetamine from another supplier into Sweden. That plan failed when in January border officials found the amphetamine in a bag in a truck. Then a couple of weeks later, Swedish police stopped another of Microsoft's transport trucks carrying kilos of cocaine. Then later that month, Microsoft tried one of his elaborate ocean cocaine drops again, this time on the other side of the world. Microsoft didn't bank on two things: the FBI and bad weather.

In late February, a ship careened through the sea fifty miles off the coast of Yakushima, a Japanese island. Just south of the mainland, the water was choppy. The ship slowed its speed, and its crew members flashed their lights three times. In the distance, a smaller fishing boat followed in the ship's wake. Through the overcast sky, it signaled back and flashed its own lights three times.

That was the sign. A sailor on the ship threw barrels overboard. After they plummeted into the ocean, one of the group sent a WhatsApp message: "29°51.9N 131°16.3E." This was where the ship had just dropped the barrels, the co-conspirator working with the crew explained. The load was full of cocaine.

The intention was for the fishing boat to then pick up the barrels and transport them to Hong Kong, from where the boat originated. The harsh weather created issues with each party not being able to properly communicate with one another. The main ship had already dropped the cocaine into the ocean, but the smaller fishing boat kept following.

"Tell them to go back not to follow us," the co-conspirator wrote.

Microsoft's fishing boat did not keep track of which country's waters it was in. Tunnel-visioned and trying to keep up, the fishing boat ended up in Japanese territory.

The FBI watched as Anom users planned this and other elaborate exchanges of drugs at sea. The operations stretched from the Indian Ocean, through to the north of Australia, and then up to Japan, China, and Hong Kong. The shipping vessel carrying the drugs would throw the narcotics overboard, and then a smaller boat would hunt out a set of buoys bobbing up and down in the water. Attached below these were barrels containing the drugs.

"The guys that were in the vessel as they're dropping their cocaine would get to the point and say, this is where we're dropping it. Here's the marker. You have the exact coordinates," Kalina said. Those markers would go to the fishing boat and, sometimes, unbeknownst to their captain, the

FBI too. The FBI jumped on these situations as much as it could when it saw an operation like this.

The agents had read plans like this before: a fishing boat would leave Hong Kong with the intention of picking up hundreds of kilograms of cocaine near Japan. Working with foreign authorities, the FBI would follow these shipments. The partner agencies would often wait until the smaller vessel had picked up the drugs before they would swoop in. So, in late February, the authorities waited. The seas got so choppy that the fishing boat could not even reach the designated drop point. The cocaine remained at sea, unclaimed.

Microsoft told others that the Japanese authorities responded to his fishing boat with a helicopter and boarded the vessel. The job ended as an expensive failure, another loss to add to Microsoft's notes. The financial pressure on him was mounting.

Back in Europe Microsoft used his international connections to land a new partnership, one that promised to turn the bad luck on his notepad around. He would source amphetamine from a lab in Holland and then sell the drugs in various European countries. The partner, Yann,[1] had experience managing multiple labs. One, he told Microsoft, churned out drugs from a brick shed in the back of a garden. The speed was good quality, and he had the capacity to ship amphetamine twice a month if Microsoft wanted. In short, Yann knew what he was doing.

He shipped a large batch of one hundred kilograms of Louis Vuitton–branded amphetamine from Holland into Sweden around the start of March. Microsoft then sold most of it in just a matter of days. That hundred kilos was more of a test run. In a sign of goodwill and to demonstrate how the pair could work together, Yann paid for all the up-front costs, including the transportation.

The shipment quickly hit a speed bump: the police managed to seize ten kilos of the cache. A loss, but not a catastrophic one. Yann absorbed the damage, and the pair carried on.

“Finnaly I have people I can work long term with thank you 😀😀😀😀😀👍” Microsoft texted Yann. Yann was in it for the long run too if everything went to plan. He wanted to work for ten years or more.

Microsoft didn’t just want the business—he needed the partnership to work. He was playing a dangerous game: his sales of amphetamine were on credit. That is, he hadn’t received any cash in hand for the narcotics. He also promised buyers batches of drugs before they had successfully arrived at their destination. Microsoft did this because he was fixated on moving the product to customers as quickly as possible rather than storing it in a safe house and then finding clients afterward. That approach, Microsoft thought, was a safer way to handle the product, less vulnerable to law enforcement raids that could wipe out his stash.

But if the drugs didn’t land, or the police seized them, that meant his customers wouldn’t get their product, and Microsoft wouldn’t get his cash. Then he would have no money to pay back any people he in turn owed money to. It was a precarious way to balance his books. His colleagues threatened to pull out; he was selling something that didn’t yet exist. Microsoft hadn’t shaken the nickname of the Fool. If anything, he lived up to it more than ever.

Those multiple seizures and screw-ups were what led Microsoft to stress over his balance sheet in the Istanbul office in late March. Debts and losses were a fact of the drug trafficking industry, and smugglers accounted for the fact that some of their shipments would get caught by customs. Or mistakes happened and people lost money. Everything worked out in the end because, generally, most shipments did get through.

This law enforcement activity against Microsoft was different. The police were incessant. Transport after transport, shipment after shipment, were gone. With every new smuggling method Microsoft dreamed up, or fresh couriers he brought on board, the police knew when and where the drugs would be.

As Microsoft grew desperate, he also grew more dangerous. He now looked to cash in on the people who in turn owed him money. After preparing for kidnappings, explosions, and hits the previous year, Microsoft was finally going to act. He still thought about the former cafe owner whom he discussed kidnapping and who owed him $800,000. He even dreamed about the target in his sleep.

Microsoft was going to kill Salah.

"Execute that guy in Stockholm," Microsoft said in an Anom message. Salah was now a prop piece, designed to shock others into falling into line under Microsoft. After killing Salah, other people who owed Microsoft money would finally cough up. He saw hiring killers as an investment, one that would yield returns when people became scared and gave him money he was owed. Microsoft might not get his money back from Salah, but others would pay. Frankly, Salah was more useful dead.

That same month, Microsoft started a group chat on Anom with Pelle Arbiv, one of his drug trafficker underlings who had helped with the earlier speedboat cocaine job, and Said Sadat, the man Microsoft tasked with organizing the hit. Sadat was no joke. He was allegedly linked to the shooting of Sascha on the Stockholm bridge the previous year. People believed he got results.

In the chat, the group laid out their options. Silenced 9 mm pistols, grenades, stabbings—everything was on the table. Microsoft was willing to pay 600,000 Swedish krona ($70,000) for Salah's killing, well above what his friends told him was the market rate of closer to $10,000.

"Do we have a deal?" Microsoft asked Sadat across Anom.

"Yeah bro," Sadat replied. "Anom is safe right?"

"100%," Microsoft wrote.

"Okay my brother," Sadat texted, confirming the contract killing.

"👍🙏," Microsoft replied.

Less than two weeks after Microsoft started the group chat, Sadat said he had an assassin ready to go. The hitman already knew what Salah looked like, and Sadat knew Salah had been at his cafe that day. Microsoft said to give the shooter an Anom and provided Salah's home address.

The last thing Sadat needed was an apartment for the killer to lie low in afterward. The target lived in the center of Stockholm; it would be difficult

to escape that area during the day. Sadat said he was checking listings on Airbnb for the hitman.

Sadat's plan was for the killer to catch Salah as he entered or left his property, pull the man inside, and then kill him with a silenced pistol. "That will give you 5 to 10 min head start, if you're lucky," Sadat said.

Arbiv riffed on that with something more elaborate. Why not have the assassin dress up as a delivery driver, knock on the door so Salah comes to answer it, and then kill him on the spot?

Microsoft loved the idea.

"The thing with delivery to the door is great," he told Arbiv in a text. "Like your style bro."

"Something we KNOW works bro 🙃," Arbiv replied.

As all the pieces fell into place, Salah's death began to appear imminent, perhaps within just a few days. The Swedish police realized this as well. As Microsoft planned Salah's assassination, the intelligence unit in the Swedish police headquarters read Microsoft's Anom messages. They saw the drug trafficker wasn't messing around. This was real, and the police needed to intervene. If they didn't, they might have another Sascha on their hands. This was their chance to correct, as much as they could, for that tragic murder.

The Swedish police only reach out to warn people they are being targeted when they deem that a threat is serious and that there is a risk of the attacker really carrying out the violence. Microsoft's planned assassination of Salah crossed that threshold.

On March 24, the same day Sadat said he was looking for an Airbnb, a Swedish police officer phoned Salah. The officer explained in no uncertain terms they had intelligence there was a threat against Salah. The officer said the authorities were taking this threat seriously. The officer didn't mention Anom, only that Salah's life was in danger.

They asked if Salah had anywhere else he and his family could stay for the time being. No, Salah said. They had spent their entire lives in Stockholm. They had nowhere else to go. In that case, at least change your behavior, the officer said. Switch the roads you more commonly use; don't go to the same places you ordinarily do.

After hearing the police officer's news, Salah's main concern was the safety of his children. Salah declined to receive further help from the police such as physical protection, like Sascha once did.

But the police weren't going to let up. Days later, they contacted Salah again. Salah had changed where he traveled to and his routines after the first call—the message had gotten through. He did mention something ominous: he had seen two people walking around aimlessly in his neighborhood.

Salah also lucked out. In the end, Microsoft and Arbiv suspected that Sadat was not prepared to go through with Salah's murder and began to explore alternatives. For the moment, Salah was safe.

Microsoft had hoped to get rich as his debtors repaid him after Salah's death. With that option now closed, he took one last shot at a big payday, one that could make up for all of his troubles. He and Yann prepared another shipment of amphetamine from the lab in Holland. The coming shipments would prove whether Microsoft could create a reliable and long-running business and change those losses on his notepad into some profits. Microsoft's main goal was to make the supply chain of drugs from Holland through to his customers in Sweden automatic, like a machine.

For Yann, it was better to send a smaller shipment each delivery than one massive batch that might get caught. However, that was not Microsoft's style. He instead wanted to flood Sweden with amphetamine. He asked Yann to whip up two hundred more kilos of drugs before finishing sales of the first batch. And he wanted this shipment even faster than the Louis Vuitton one. This time he asked Yann to stamp it with the word "TJACK." (When Microsoft asked for a four-letter stamp that spelled TJACK, his new partner pointed out that word used five letters.) The stamps Microsoft requested were only to be used for his drugs, his calling card. Yann's kitchen staff dutifully made a stamp out of wood to be pressed into the blocks of amphetamine. The plan was for TJACK to be the best on the market in the whole of Sweden.

When the FBI saw Anom texts mentioning TJACK, they contacted their Swedish colleagues: What does this word mean? The FBI also asked about what they thought was the "salmon" case when that word appeared in their logs. The Swedish police explained both were slang. There was no salmon case; "salmon" meant an amount of money. After multiple misunderstandings, and the Swedish police laughing, they provided a breakdown of other terms, such as "apple," referring to a hand grenade. TJACK, it turned out, was a common Swedish word for speed.

In early April, a truck from a flower company carrying the first 120 kilograms of Microsoft's TJACK crossed the border into Sweden. The drugs arrived at the safe house, and Microsoft's couriers started to distribute the speed. Almost predictably by this point, the police struck again. They seized eighty-five kilos. The TJACK had been in the stash for just a few days.

"Back to square one," Microsoft wrote on Anom, defeated. Not wanting to lose momentum, he asked an associate to send another sixty kilos. Microsoft was demanding more and more drugs without realizing the police could read his messages and grab any new shipments as well. He was trying to outplay an opponent who would always know his next move, and always know where to strike.

After this second seizure, Microsoft's relationship with Yann was strained to a breaking point. Yann had been okay splitting the loss for the Louis Vuitton speed the police grabbed in March. Now Microsoft wanted to divvy up the damage for the police discovering his stash house and taking eighty-five kilos. Yann was less forgiving this time. He would not absorb the financial hit. That was Microsoft's problem. This arrangement was pitched as a partnership, but only one side was stepping up. Yann made it clear: if Microsoft didn't sort out payment soon, he would not ship any more amphetamine.

Ashamed and driven to a new low, in a desperate scramble Microsoft begged a contact to help him out with money.

"Please bro, just this once," Microsoft said in one Anom voicemail, his voice stuttering. "I won't say anything. You… you'll get to know me bro. Just these two weeks about this loss you know."

Two days later, Microsoft managed to send Yann some money: a lousy 8,500 euros.

“What is this a joke??” Yann snapped back on Anom. “This is child play.”

Microsoft’s partnership with the lab manager wasn’t the only relationship falling apart. Even his other contacts didn’t want to sell his drugs anymore. Something about this speed was cursed.

“Bro I don’t want any more tjack,” one wrote.

“Please bro,” Microsoft replied.

“Bro the arrangement is not good,” the associate continued. “Think for yourself bro. We are supposed to make money selling his drugs on our risk,” they wrote, referring to Yann.

Inside the Swedish intelligence unit, Microsoft’s steady fall from grace was a source of great entertainment. When the smuggler admitted in Anom messages that he had never heard of a drug trafficker losing multiple shipments in such quick succession, smiles spread around the office. Analysts gossiped among themselves: “Have you seen this? Have you seen what Rivkin sent?”

On April 13, about four days after the TJACK seizure, Microsoft had the blinds drawn and his laptop placed on a blue sofa at just after eleven p.m. He rapidly flicked through different spreadsheets that tracked his drug income and outgoings. Microsoft’s situation had been bad when he scribbled figures onto his notepad in March. Now it was on a knife’s edge.

Microsoft’s crew wasn’t the only syndicate that felt something was amiss. Elsewhere, Christof’s clients grew suspicious of Anom. As soon as one of them started using Anom, police seized a drug shipment of theirs. Anom was jinxed, the customer said.

Recently, an anonymous tipster had also created a website called “Anom Exposed” that claimed Anom was funneling user data to law enforcement in the US. Anom determined it was the work of a rival phone seller trying to stir up rumors. But the post still sent Anom customers into a paranoid frenzy.

Arbiv directly asked Microsoft the question that was appearing on more and more people's lips: Were these seizures because of Anom? Was Anom compromised? A day later, another associate pointed the finger at Anom: maybe the police had found a way to read Anom's messages? Then in less than a week more people Arbiv knew in the Swedish city of Gothenburg were caught by the police. They were only using Anom to communicate.

Oblivious to how thoroughly infiltrated his operation really was, Microsoft dismissed each warning. Besides, people in the crew were still out of prison. If Anom really was compromised, wouldn't everyone be behind bars by now? Instead of the phones, Microsoft fixated on his couriers and stash handlers. A member of the crew must have screwed up.

To try to assuage users' growing fears, Microsoft provided Arbiv with boilerplate text that he could pass on to the trickle of criminals now suspicious of Anom.

"Cybersecurity is an arms race. Anøm is constantly developing the platform to stay ahead of current threats. Any vendor that can guarantee that their system cannot be broken into is selling snake oil," the message, not at all in Microsoft's usual style, read. As a final reassurance, Microsoft stressed that Anom was run by criminals. Why would a company run by criminals, designed to protect criminals, let the police read its users' messages?

Microsoft might have genuinely believed Anom could not be compromised. Or perhaps that was a possibility he didn't want to even engage with. His blind faith was so strong that when his most trusted advisers brought up Anom again and again, Microsoft did not listen. To him, Anom was never the problem, despite months and months of raids against his and others' businesses. It was as if everyone knew something was wrong with Anom except Microsoft.

Microsoft, like the monkeys tattooed on his arm, had his hands covering his eyes and ears.

Footnote

1 Author has changed this person's name.

Chapter 28

Green Light

In October 2020 Bobbitt, the FBI assistant legal attaché, was in the secure communications room of the US embassy in the Netherlands, a windowless space with loud computer servers. On a call with Cheviron and Stevens from San Diego, the agents needed to find a new plan.

Cheviron and Stevens wanted to enter the next phase of Anom: a much wider span of collaboration beyond the Dutch, Swedish, and German authorities. The agents wanted to bring their current European partners and representatives from many more countries to San Diego to work together on Anom in person. In person, the consortium of agencies could ramp up their seizures of drugs and weapons and more easily stop planned assassinations. Together they could formulate what a final takedown of Anom and a massive wave of arrests might look like.

With the French hack of Encrochat in 2020, the harvested data was stuck in a bottleneck, with only a few select agencies able to properly rummage through and act on it. Bobbitt compared it to "one guy processing every Amazon Prime" order.

The FBI didn't want that. Instead, they wanted to get as much data into the hands of a large selection of agencies as quickly as possible. Rather than handing out the data piecemeal, they envisioned giving many more countries direct access to Anom's chat review platform.

But the current plan would not work. The US border had essentially been closed to travelers since March and remained locked down. Any foreign partners simply wouldn't be able to get to San Diego.

On the call and multiple others, Cheviron and Stevens worked with Bobbitt and more legal attachés to see if the FBI could find an alternative location to bring these agencies together. COVID-19 was still a complicating factor, but soon the FBI asked the Dutch if they would be willing to host such a collaboration. The Dutch said no. The Germans said no too. As did the Swedish. Veronica Urve, head of unit at the Swedish Police Authority's Department of National Operations, told the FBI that Europol really was the best place to bring these agencies together.

Europol was the European Union's law enforcement coordination body. Based in The Hague, Europol was a central repository for intelligence gathered by European agencies and a hub that could more easily put each agency in contact with another. Maybe here, the FBI and its foreign partners could work on Anom.

Immediately, Bobbitt had a long list of concerns. He was worried Europol wouldn't be able to keep it secure; that the FBI wouldn't be able to lead the operation if it went there; and that the whole thing might drown in Europol's own bureaucracy. But he wanted to gauge Europol's interest.

Instead of formally proposing the plan to Europol, Bobbitt went to a contact who had become his best relationship at the agency. The contact was excited and said the FBI should bring Anom to his agency. After some back and forth, the contact texted Bobbitt in the evening.

"Do I have the Green Light for tomorrow?" he wrote, asking if he had permission to tell his superiors about the plan.

"You have the Green Light," Bobbitt replied.

"Copy."

Soon, Bobbitt was in a meeting at Europol with the contact, as well as Georgios Raskos, the head of the Organised Crime Unit, and his boss Jari Liukku, the head of Europol's European Serious Organised Crime Centre. The Europol officials at the meeting assured Bobbitt they would put 100 percent of their support behind the operation.

Technically, the FBI could not run such a program, called an Operational Task Force (OTF), at Europol. The US was not a European Union country. The solution was that the two EU partners already making great use of the data—the Netherlands and Sweden—would cofound the OTF. Each country had to designate a high-value target as part of that process. Sweden picked Microsoft.

The FBI and Europol still needed a name for their new task force. Sitting in the basement of Europol over coffee, Bobbitt's contact threw back to their earlier text exchange: What about Green Light? I love it, Bobbitt said. For the code number to go along with the name, Bobbitt chose 324—the FBI's letters on a phone touch pad.

Over several months, the FBI, Europol, and Swedish and Dutch authorities prepared OTF Greenlight. Cheviron and Stevens traveled between the US and Europe to manage the now even larger operation. The FBI invited a huge array of other countries: Canada, Denmark, Estonia, Finland, Hungary, Lithuania, New Zealand, Norway, Scotland, and the United Kingdom (Australia was also a member of the task force although they were already neck deep in Anom data. Austria joined later).

"The great part is that most of the countries that those devices went to, were sitting there in Europol with us, and participating with us," Kalina recalled.

Europol wasn't allowing visitors, and if someone did not have diplomatic status in the Netherlands, they could not travel to the country. Eventually, Cheviron, Stevens, and Kalina from the FBI were able to get in, after some juggling from the US embassy there. The agents' presence, and the bustle of activity in Europol, raised questions from other liaisons. Bobbitt would have to say, sorry, that's not something I can talk about, even when speaking to some officials from countries whose members were in the OTF.

As Anom absorbed Sky's migrating user base, criminals didn't just unknowingly run into the FBI's hands. They now strode into the reach of their respective domestic law enforcement agencies too—the ones that could actually arrest people in Europe and elsewhere.

After officials from each country arrived at Europol in March 2021, they made a startling discovery. On floor A-2 of Europol's headquarters, the representatives sat in small offices with two desks each off a long corridor. Each country's flag was perched outside their respective door. Officials could simply walk across the hall to speak to their counterpart from another country. In the middle of the floor was a refrigerator and coffee area, along with tables and a large projector. Europol analysts who dug through the data sat in their own larger bullpen at the end of the hall. Much of the

rummaging happened back home by each respective country's analysts, who then provided updates to their representatives in Europol.

After a long day of working on Anom intelligence, an official would often bring out a bottle of their country's local vodka or brandy. The startling discovery was that there were only security cameras in the hallway and common area, and not inside individual offices. The group figured out which offices they could be in while out of the line of sight of the cameras. This meant they could gather and drink without Europol's security guards telling them off for breaching COVID-19 precautions, which happened repeatedly. The officials also poured their booze into coffee cups to remain undetected.

Like the San Diego FBI's empty hotel, Europol was otherwise closed because of COVID-19. No other operations were ongoing at the facility, and because the cafeteria was deserted, the officials emptied out a vending machine every night or brought in their own food. Bobbitt had far too many hummus wraps, he said. Even then, officials were still careful to not speak specifically about Anom when around the coffee machine. That way, when outside the confines of floor A-2, they would be much less likely to let anything slip.

Every day at nine a.m., the FBI hosted a briefing inside a large conference room at Europol, each person spread out to maintain social distancing. Cheviron, Stevens, Kalina, or Bobbitt would run through how many messages were in the latest data dump, how many more people had signed up to Anom, and how large the network was overall. The agents spoke about new functionality being added to the Anom phones. The FBI also highlighted emerging issues it saw in the Anom intelligence, like the global increase in 3D-printed weapons—where rather than buying guns, criminals manufactured them for relatively cheap—or an uncovered drug smuggling technique. The FBI also met with individual countries if any new syndicates on Anom impacted them specifically. Sometimes the briefings could drag on for hours.

Then there were the negotiations. At a roundtable every country said whether they planned a seizure. Here, the FBI and their partners discussed whether it was wise to jump on a particular cache of narcotics or not. Anom was too valuable a platform to burn over a small shipment of drugs. Sometimes the negotiations ended on a compromise: an agency could work

with another country in the task force to seize the drugs later, after they had crossed a border. That way, it may not have been so obvious that Anom was the source of the leak.

Urve from the Swedish Police Authority said Swedish authorities sometimes let smaller drug shipments they had intelligence on go ahead. “If we take another one now, it would jeopardize everything,” she said. Urve also had to tell white lies to her own colleagues. At one point, a Swedish officer prepared to raid a warehouse and phoned Urve to ask about the intelligence. If the raid went ahead, would Urve’s source be in danger? he asked.

“Give me ten minutes; I will just check with my source and get back to you,” Urve replied. She hung up the phone and pretended to be busy for a short while. She then phoned the officer back and chatted some more, all the while not revealing the tip actually came from Anom and instead implying it came from an informant.

“He actually thought my source was in danger. I felt a little bad lying. I had to do it to protect the whole Anom case,” Urve later recalled.

Frequently, Europol officials asked the FBI for Anom intelligence on somebody they were investigating outside of the OTF. In one case, a load of drugs was coming into Croatia, a European Union country, but one that wasn’t part of the task force. We need information right away, this is urgent, the officials said. The high priority requests became so regular that Bobbitt and the other FBI agents grew a bit numb to them.

But in May 2021, Bobbitt’s Europol contact had a different look in his eye when he asked for help. I need you to look into this guy, he told Bobbitt. “Morabito,” he said, uttering only the target’s last name.

Bobbitt had never heard of this person. Neither had Stevens. But Morabito was the real deal. Unbeknownst to them at the time, Rocco Morabito was a top-tier ‘Ndrangheta figure. He was on the run after escaping from a Uruguay prison in 2019 while awaiting extradition, and Italian authorities had ultimately been hunting Morabito for decades. Morabito was the number two most wanted criminal in Italy.

Bobbitt and Stevens dug through the intelligence, and, sure enough, an associate of Morabito’s was using an Anom phone. Through messages that person sent to someone else, it became clear the pair were making plans to travel to Brazil. They were planning to visit the boss. Morabito.

Authorities already suspected Morabito was in Brazil. But now the FBI had a tip on a duo who could lead them right to the man himself.

The messages indicated the men would fly from either Germany or the Netherlands to Brazil within the next several days. Bobbitt passed information to his Dutch contact, who obtained flight manifests and confirmed which flight. The Brazilian authorities, Italian police, US DEA, and FBI hatched a plan.

After the men landed in Brazil, a local team on the ground followed the Mafia members from the airport to a hotel. One of the men then walked over to where Morabito was at a beach resort. The team spotted him and immediately made an arrest. They got the mafioso.

"It looked like the simplest thing ever. On the ground, it just looks like they happen to find him at the airport and follow him directly to Rocco," Bobbitt later recalled. The behind-the-scenes truth was that the FBI's ownership of Anom led the authorities to Morabito.

Back in Europol, the FBI agents walked into the OTF, and everyone who knew about Morabito was excited. One Europol contact told Bobbitt the news. They got him, they got him, he said. That's great, both Bobbitt and Stevens replied, and then a second and a half later went back to work. There was simply so much to do that even capturing a top Italian Mafia member didn't provide ample time for a celebration.

The episode led to plenty of questions from the Italians, who weren't part of the OTF and had no idea about Anom's secret. Why is the FBI telling us that this guy is flying from the Netherlands to Brazil? Ultimately, it didn't matter. Morabito was in custody.

As Anom continued to grow and the OTF handled more data, the daily meetings increased, with another at five p.m. Then, at eight a.m., noon, four p.m., and six p.m. And in between and after those, the agents went back to their offices to bang away at the intelligence again.

That nonstop loop of threats to life and massive drug shipments led to an underlying problem. Bobbitt and his superior joked they had to keep Cheviron and Stevens alive. They were only half kidding. Cheviron and Stevens were the driving force behind the operation, especially as it entered this new phase at Europol—they had built the personal connections to other agencies, the understanding of the tech, and along with Young earlier had brought this crazy idea to reality. Now they were the ones managing the

largest sting operation in history. “Without them, it would have fallen over. And I don’t think either one of them could have done without the other one. I don’t think that would have been possible,” Bobbitt said.

Sometimes Cheviron and Stevens only slept four hours a night. They skipped meals. When Cheviron would get mad for no apparent reason, the other agents would laugh at him because, more often than not, he was just hungry. Bobbitt or Stevens would hand him a banana, or Bobbitt would go to the vending machine (the vending machine cookies were very good). Cheviron would laugh; yeah, I need a snack.

Stevens, meanwhile, gave birth earlier during the operation. After she joined Cheviron and Bobbitt in Europol, she had to find a way to store and ship her breast milk back to the US, all the while dealing with the unrelenting torrent of Anom messages. (Bobbitt made sure Stevens had a pump at Europol and learned it was possible to send frozen breast milk from the Netherlands to California; the FBI helped ship it.) In between meetings or during conference calls, Stevens sometimes ran off to pump.

If the duo had a nervous breakdown, or physically succumbed to the operation, Anom might crumble too. So Bobbitt said he made sure to take care of the duo. He took them to the US embassy’s gym for workouts. He checked that Cheviron and Stevens ate well.

Perhaps most importantly, the agents soon settled into a ritual of sorts: gin and tonics on Bobbitt’s back patio a two-minute drive from Europol. With restaurants closed and nowhere else they could go beyond Cheviron’s or Stevens’s hotel rooms because of COVID-19, here they decompressed, brainstormed, and planned the day ahead. In what started as a one-off hangout, those nights eventually started later and later, and ran on later and later, Bobbitt said. They became a necessity.

The map of Europe Jari Liukku, one of the Europol officials Bobbitt met with earlier, had on his office wall grew less and less relevant by the day. Each country was in a different color to give the impression they were distinct from one another. But the artificial lines that separated each nation

from its neighbor meant very little to the criminals Liukku's staff helped catch. If criminals weren't going to pay attention to borders, law enforcement needed to respond with its own version of cross-border collaboration, like OTF Greenlight.

Liukku and his colleagues first worked with the Encrochat data. Then, the Sky messages. Finally, Anom came to Europol. This triple whammy of encrypted phone investigations gave even seasoned law enforcement officials like Liukku an unprecedented insight into how top-tier gangsters worked in the 2020s. Liukku's main takeaway was it didn't make sense to talk about organized crime groups anymore. That was an antiquated idea, from when crews stayed within their regions and worked as self-contained units. Now, with his deep-set eyes, Liukku saw organized crime networks. Mexican drug specialists came to Europe to run cocaine conversion facilities with local collaborators. Albanian gangsters injected themselves across the whole drug supply chain. Money launderers sifted and sorted money throughout the entire continent and beyond, acting as connective tissue between multiple gangs.

"We had Sky ECC and Encrochat investigations actually ongoing at the same time. As a combination of the information from these major operations, connected with Europol analyzing systems, we started to see really the whole scope of the organized crime networks," Liukku later recalled in his gruff voice. These networks were so fast moving that some of the intercepted material could already be stale. Liukku had the hopes of a more permanent solution. "It's good that we have this type of investigations, but actually, we should have them all the time," he said.

Taking the data together, Liukku and his colleagues now had a deeper understanding of the size of organized crime in Europe. And it shattered their previous assumptions. In 2016, Europol estimated the value of proceeds of crime in the European Union was a minimum of €110 billion ($122 billion). "I think that we can triple that amount to get a bit closer to the reality," Liukku said.

Kraag from Politie compared the harvesting of organized crime's encrypted communications to when Allied Forces cracked the Nazis' Enigma code in World War II. The tabletop Enigma machines scrambled the Nazis' most valuable secrets. When Polish and later British cryptologists deciphered the messages, it provided the Allies with an incredible bevvy of

intelligence. In that history-altering case, the Allies had control over the communications of their enemy. The espionage won the war. (In an even closer analogy, the CIA secretly took ownership of an encryption company called Crypto AG, which provided cryptographic tools to various countries. The CIA and West German intelligence worked together to backdoor the company's products.) Now, in a bold new age of policing, cops did the same outside of wartime. Cracking encrypted phone networks was the twenty-first-century way police were going to beat, or at least hamstring, organized crime.

"If you have control over the communications of these criminals, you have control over these criminals," Kraag said. "You're in front of the game. You know what's going to happen."

Through its years of encrypted phone investigations, the Dutch police found a way to comprehend mountains of data. They developed artificial intelligence programs that ingested the messages, interpreted what was being said—such as this conversation being about cocaine—and then provided that result to the analysts. This meant humans didn't have to painstakingly read every message. They could instead focus on those that the AI system surfaced for them.

As part of the new international collaboration across Anom, the Dutch police made this capability available to Europol. Politie had never gone as far as to run their own encrypted phone company, though. That was a step up even for them.

Soon, a fundamental problem with running a successful tech company emerged. Every time the FBI made progress up the mountain of Anom messages, it grew in size, again, in front of them.

Chapter 29

Hydra

Room 2022 of the San Diego FBI's field office, a large command center with windows that overlooked the lush valley below, was now a hive of activity. Rows of agents streamed through Anom messages as the sound of overflying jets sometimes hummed through the walls.

When Anom produced too much intelligence for the San Diego FBI to digest by itself, it put out a call to other FBI field offices: any willing agents, at any job level, please come to San Diego and dig through Anom's contents with us. The largest request was in fall 2020, but the agents made repeated calls for help. Superiors signed off on the request for more resources.

Word of Anom quickly spread around different FBI squads. Soon a rotating cast of around 130 agents worked through the messages. Some tapped in remotely over Hola iBot, while many flew across the country to San Diego for the chance to work on a unique operation. For thirty to ninety days, day in, day out, these workers did nothing but review and disseminate the Anom data. Some stayed longer. The California weather didn't hurt.

As well as room 2022, agents used other spaces across four more floors of the FBI building. Similar to the ongoing task force at Europol, each room at the San Diego FBI had a daily briefing, and sometimes the agents held larger gatherings outside in a patio area with a barbecue. So many people were now involved that agents spilled onto the nearby lawn.

The FBI needed that help fast. Every time more Anom devices came online, Bobbitt remembered Cheviron said the same thing: We can't do this. Anom is too big. It's just getting too big. It's going to break. Anom was

constantly redlining, teetering to the edge of imploding, and then the FBI would get more analysts or another country would help out. Then the cycle repeated.

The FBI had created a rampaging, multiheaded hydra that the agents wrestled to keep under control. Resellers expanded into more countries still, including South Africa in late May. The portal meant Anom's dealers continued to push quickly and aggressively. Ayik and Microsoft cloned black boxes as they pleased.

The FBI's hands-off approach to Anom's day-to-day business meant that the agency hoped it couldn't be called out for entrapment. The FBI had safeguards in place meaning it could pull the plug on Anom if it needed. At the same time, the agency had handed over power to entities outside the FBI, like Ayik, and those people were driving Anom now.

Come May, Bobbitt saw Anom could not last forever. Buckling under its own weight, Anom produced more intelligence than ever before. Bobbitt said thirty new syndicates joined the platform around every other day. Up until the closure of Sky, Anom had something like five million messages in total. That jumped an order of magnitude to twenty-two million after Sky's downfall. In some cases the FBI harvested up to a million Anom messages a day in forty-five different languages. Anom's distributors sold a total of around twelve thousand phones.

In one call with headquarters, the FBI agents told a superior just how large Anom had grown. "He lost his mind," Bobbitt recalled. Why are there so many devices on the platform? How did this happen? What am I going to tell executive management?

"I don't think they ever thought it would get to the point that it did," Bobbitt later said of FBI higher-ups. "And it scared them." Anom was too successful, and the FBI found it hard to keep up with the company's monstrous scale any longer.

The mountains of messages included around twenty-five hundred pictures per data dump, all of which the analysts had to review for threats to life. When the FBI and its partners stopped one act of violence, the criminals immediately texted across their Anoms: How the heck did the authorities know about this plan? "We would smile and laugh about how they didn't figure it out," Kalina said.

Those cheery moments quickly passed. Because many of the criminals still didn't yet suspect the devices, they pointed the finger at the next most likely thing: each other. And when violent criminals think that one of their co-conspirators is a rat, they kill them. The FBI then had to find a way to protect the second person who was threatened. And so on. The spiral of threats went round and round, with no clear end to the violence in sight.

"Now we have another threat to life, and now we gotta protect one of their bad guys, because they jumped to a conclusion that was completely wrong," Kalina said.

In all, law enforcement estimated that it intervened around 150 times to stop a threat to life. Given that loudening drumbeat of activity, the FBI knew its customers would figure out Anom's secret eventually.

The FBI always wanted Anom to end at some point. Up until now, Anom had mostly been an intelligence tool, used to provide tip-offs about drug shipments. Now it was time to change Anom to an evidence-gathering tool, one that could be used to prosecute those drug traffickers in court. Soon the authorities could finally go loud and make a mass of arrests of Anom's users, including many of the high-value targets they had been tracking, with the potential to majorly disrupt organized crime around the globe in one giant hammer strike.

Even more importantly, the FBI and prosecutors had a broader overarching goal: to shatter criminals' trust in the encrypted phone industry. If the FBI was willing to secretly run an encrypted phone firm itself, what was to say that any of the other companies weren't also law enforcement honey pots? With that paranoia, the FBI hoped gangsters may abandon the industry altogether, and leave behind the sort of technology that had protected them for years. That undermining of trust could only be achieved if the FBI came out and publicly admitted it owned Anom.

A natural end sat on the horizon: in June, Lithuania's court order, the legal glue that held the whole operation together, would expire.

Cheviron and Stevens told others a firm date: June 7. This was the day Anom's true management would step out of the shadows. The FBI would reveal it was the secret puppet master of Anom. The international partners, the consumers of the data, wanted the FBI to keep Anom going. But there would be no negotiations; this was the time to stop.

With the bustling work in San Diego and Europol, the Anom operation entered a new, never before seen scope. Members of OTF Greenlight investigated at least eight hundred people they were prepared to arrest. A nearly unfathomable surge of activity from agencies spread around the world, all coordinated with the FBI at the helm. The activity went beyond the analysts sitting behind computer screens and involved many more officers in the field. The agencies built cases on those suspects. As good as the Anom messages were, they weren't necessarily enough to guarantee a conviction. Investigators combined the messages with physical surveillance, data from social media, and ordinary phone companies. They built a rich picture of who exactly these Anom users were, where they dealt drugs, where they slept.

Then in some cases the agencies took action, like the Swedish police had on Microsoft's organization. In May Dutch police uncovered intelligence on a cocaine processing plant inside an apartment complex above a daycare center in Amsterdam. The process for refining the cocaine was very volatile, putting the nearby children at risk. Dutch authorities asked Bobbitt if they had permission to strike. "Of course," Bobbitt said. "We hit it, and we hit it right now." Authorities arrested four men from Amsterdam, Albania, Ecuador, and Colombia who tried to flee on the balcony and roof.

Australian authorities, too, went on the quiet offensive. All across the country, state, border, and federal police picked up drugs and weapons throughout April and May. More investigators from regional police forces were looped into Operation Ironside. Embedded with the AFP in Sydney, they ferried intelligence back to their respective state agencies.

In Queensland to the northeast, police seized a semiautomatic rifle from a criminal syndicate. Queensland Police also found several ecstasy labs and shut them down. Authorities stopped shipments of meth from America hidden inside hard drives. The police removed the drugs, delivered the packages to their expected address, and arrested a man who relayed the packages to a safe house nearby. Inside, the cops found more drugs and a mobile phone jammer.

Then in New South Wales on the east coast, border officials stopped more shipments from America, such as a kilogram of cocaine coming into Sydney. The group was reportedly linked to Ayik. The AFP and NSW Police found 230 kg of cocaine hidden inside machinery from South Korea.

Authorities then found 270 kg of methamphetamine, also hidden inside machinery, stored in a factory. Police busted two money launderers who were holding on to over $1 million, then another who had $1.5 million.

In a southern corner of the country, the AFP tipped off local police about a cash drop. Victoria Police stopped a car and found what they estimated to be $250,000 in three vacuum-sealed bags. In a second case, they discovered $700,000 in a blue suitcase after searching a target's house. Victoria cops stopped another vehicle and found duffel bags of cocaine and meth. Victoria's Drug Task Force also worked with intelligence that led to a clandestine lab for producing MDMA.

In South Australia, police seized fifty kilos of methamphetamine hidden inside a truck at a port. The officers knew exactly where to look for the drugs thanks to data from Anom. But to keep Anom's secret under wraps, authorities took the truck to be X-rayed. They could claim that was how the drugs were discovered if anyone asked.

Finally in the west, state police seized nearly $1 million from a man and two women who laundered cash on behalf of a biker gang. West Australia police also found a dozen kilograms of meth inside a roof cavity. Anom directed state police to a dead drop in the hills near the city of Perth. Police found three kilos of meth there and swapped it out for an innocuous substance. When a woman arrived and dug up the bag, the police pounced and arrested her. In another search police found a cornucopia of drugs hidden under an oven.

These busts impacted a wide range of different criminal syndicates and outlaw motorcycle gangs. No one criminal had visibility into all of them. If they did, maybe they would have identified the pattern: all of the targets used Anom. Since the start of Anom years earlier, Australian authorities had arrested around a hundred people out of the more than sixteen hundred who used the phone in the country, all the while keeping the ultimate source of their intelligence a secret.

Still, the Australians might have gone too far with this flurry of activity. Criminals started to circulate rumors that Anom was compromised in some way. In May police arrested multiple drivers who allegedly worked for an Australian individual called George Katsambas, who Australian authorities believe is linked to criminal activity. He told friends he was going to Greece for three weeks. Shortly before his exit, he messaged an associate, "Bro,

someone told me today that AN0M is bad." Authorities then arrested Katsambas at Sydney Airport.

Although the FBI wasn't going to be arresting anyone itself on June 7, it drew up its own list of targets. The prosecutors wanted to add a cruel twist: they were going to charge the very people who had made Anom popular with criminals across the world. The FBI set crosshairs on more than a dozen of Anom's top sellers. The job of preparing the indictment fell to Meghan Heesch and Joshua Mellor, two prosecutors from the US Attorney's Office in San Diego. Around the globe, those sellers felt the effects of Anom, seen and unseen, surround them.

One afternoon in late spring, Christof, Wijzijn, and a handful of other European Anom sellers sat down for lunch on the terrace of a Spanish seafood restaurant. White umbrellas sporadically covered the outside dining area. Everyone ordered fish, and most of the group was hungover from partying the night before.

As the group ate and chatted about Anom's ongoing expansion into Russia, a car parked on the road next to them, its front pointed in the group's direction. That was unusual. No one parked there. If you did, a tow company would probably take your vehicle away. Cars were not allowed to stop in this mostly pedestrian area of the city.

Two men in khaki jeans and T-shirts stepped out and walked away from the car. Christof immediately thought they were undercover police. The vehicle was so close that if a camera were inside, the cops could get good photographs of the various Anom sellers together at once.

The group was not impressed. They all thought, "Why the fuck did they park there? These shit undercovers," Christof later said. The men returned to their lunch and parted ways after a couple of hours.

This wasn't the first time that Christof had seen what he believed were undercover police tailing him recently. His Anom clients had also noticed suspected police officers monitoring them.

At one point Christof was having beers with a client in a bar. A man then entered the bar, sat down near the pair, and repeatedly pointed his smartphone at them. In another case, Christof was selling a phone in a city's commercial center when he noticed someone repeatedly looking through the windows at him.

"You hang out with a certain type of people, you get this monitoring every now and then," Christof later recalled. But this was different. In the lead-up to the restaurant meeting, Christof saw suspicious people on what he felt was a daily basis.

"Something's not right," Christof told his wife afterward. "Something's going to happen soon."

In Australia, contacts of Catanzariti, Anom's first seller, were thinking of quitting the criminal life altogether. In May the AFP, among many other operations, tailed members of the group and found multiple kilos of meth hidden inside a Ford Transit van and a set of trash bins. Through Anom, the AFP had also found drug smugglers used waste management services to retrieve narcotics stashed inside bins in ports.

The AFP arrested two of those gangsters. Panic started to set in.

"I'm not doing this anymore to [*sic*] much risk and to [*sic*] much to deal with," one member wrote. He hadn't slept all night and felt physically sick. One day later, another member noticed the police hadn't yet put the arrest on the news. A deafening silence from the authorities while more and more people were quietly picked up.

Meanwhile in Turkey, Microsoft was consumed with his worst anxiety yet. Everything from the past six months—the amphetamine lab raid, the failed Hong Kong job, the Louis Vuitton and TJACK seizures—had built up. It

had finally all taken its toll on Microsoft. His skin broke out in rashes from the stress. He simply did not understand how he was in this situation.

Then near the end of the month, he lost another fifty kilos of amphetamine. Swedish police tailed some associates of the violent Bandidos biker gang that Microsoft had worked with and found the drugs.

That seizure was the knock-out punch.

In an Anom voicemail he opened up to an associate about his dire finances. After this latest seizure, he was now in the red and wouldn't have any money for the next six months. Microsoft had gone from someone who orchestrated twilight drops of cocaine by speedboat to a rash-covered mess. His partners, some of whom even discussed killing Microsoft, were sick of working with him. His own finances were dwindling. And the police seemed to be a step ahead of him every time. Microsoft's world fell apart around him.

"Count me out as zero, zero, zero. Have no money, don't have anything. I don't know what to do with myself," he said. The Swedish gangster didn't yet know the exact cause of his serial misfortune, but Anom had driven him into the ground. The very tool that he thought would help protect him in the drug world aggressively ate away at first his business and then his health.

Ayik, who continued managing Anom, was about to expand the company even further. He managed to convince the biggest distributor of phones from No.1 BC, a rival firm, to soon drop their company and join Anom. This seller allegedly had another whopping customer base of ten thousand users, the equivalent of around double Anom's user base, again. Whispers of that acquisition trickled down the Anom ranks, with some sellers excitedly telling their colleagues about the news. As of Friday, June 4, just days before the FBI planned to go public, Ayik plugged away at an internal Anom spreadsheet. He had no idea what was coming for him.

The FBI agents were already barely clinging on to Anom's ballooning size. They could not handle another influx from Ayik's latest business deal. The dam would simply burst.

The agents just needed to fool Anom's users for a few more days, when the authorities would finally move to arrest as many as they could. If too many figured out Anom's secret, they might go on the run.

And every day that Anom stayed online, the chance of authorities missing a crucial message, and someone being killed as a result, only kept increasing. Anom was a pressure cooker, shaking more and more violently.

Chapter 30

Mancuso Luck

Former Lone Wolf biker Dillan Mancuso was fast asleep at around three a.m. on June 1, 2021, dressed in just a pair of translucent white underpants and his tattoos. “What goes around comes around” encircled his pudgy stomach in a gothic font. His collarbone read “Unstoppable.” His back brandished a giant cross, and “MANCUSO” was printed across his shoulder blades. That was the then thirty-seven-year-old Mancuso to a tee: loud, brash, and very cheeky. Throughout life, he always managed to land on his feet, what others called Mancuso Luck.

He was staying in his father’s terracotta-roofed bungalow in Bringelly, a rural Sydney suburb where well-spread-out homes stood along a long, straight road sidelined with palm trees. Four-foot-high fences sat between each house.

The bungalow was packed, with another five members of the family all sleeping too. Authorities had granted Mancuso bail to come to the area for a wedding. The real point of the trip was to see his young son, one of those five. Mancuso was only staying in the bungalow for one night before he returned back to Perth, on the other side of the country.

As well as being a user of encrypted phones, Mancuso had sold phones for Phantom Secure during the company’s Australian heyday. Later he switched to other companies. Now years later as part of his bail, Mancuso said he was not allowed to have a Ciphr phone, even though the encrypted devices were still popular in Australia. So, he bought a handful of Anom devices instead. One for a friend, one for his girlfriend, and one for himself. As soon as Mancuso started to use his phone it broke, before he had used it

to plan any serious crimes. Mancuso brought the broken Anom with him on the wedding trip to have it fixed. That night it sat in the open on his bedside table, apparently back in working order.

This bail was just the latest episode in Mancuso's life in and out of prison. He said he was previously convicted when a drug importation went south. At first prison was daunting, but he came to enjoy some of his stints in jail. It was like being back with the boys at summer camp—when he wasn't deep in beefs with bikers. In late 2020 as part of an investigation into an alleged drug trafficking ring, Australian authorities seized two Mercedes Benz automobiles and a Bentley from Mancuso and his girlfriend at the time. The cars were worth more than $100,000 each.

Even though he was charged with possessing suspected proceeds of a crime, Mancuso wasn't bothered by the car seizures. He fobbed them off as chump change. Which might have been why rumors circulated about his true wealth. Maybe he had more money stashed away.

Joe, Mancuso's father, woke up when dogs outside started barking. He made his way to the lounge, sat down in his armchair, and put on the TV. Joe drifted back to sleep.

Suddenly, a bang shook the bungalow. The noise was so loud that Joe thought a car had crashed into the house. He jumped up and ran to the front door. But Joe saw there was no door left: it had flown off its hinges and now lay on the ground.

Through the gaping doorway strode multiple burly men in balaclavas, hoodies, and sweatpants, more than a half dozen of them. The biggest carried a handgun.

Joe thought they must have the wrong house. "What's going on, fellas? What's going on?" he asked. "You got the wrong place, you got the wrong place."

The biggest of the men belted Joe with the butt of the gun. Then hit him again. A second man then shoved Joe into a corner and pushed his head against the wall. "Don't move, just put your head there, and don't look," the man ordered.

Joe was fine taking the beating as long as the group didn't hurt his family. Blood gushing from his face and head held to the wall, Joe strained to see what was going on.

Joe's daughter and her boyfriend came out of their room. They saw what was happening and immediately ran back inside. One of them locked the door, and the men kicked it a couple of times. Joe's elderly mother somehow didn't wake up as the invasion continued.

Then the men found what they were looking for: Dillan Mancuso. They dragged Mancuso, still dressed only in his underwear, through the house and then onto the pebbly driveway where two cars were waiting. Before they left, one of the men grabbed Mancuso's Anom phone from the bedside table.

"Where you taking him?" Joe said as the men started to leave the house.

"Just don't look. Don't call the cops," one of them replied.

Outside, the gaggle dragged Mancuso toward one of the cars. In the scuffle, Mancuso managed to break free and started to run in the pitch black. It wasn't clear where he could actually escape to, but he kept on going.

Mancuso turned around to see how far he had managed to get away from his pursuers. A sizable gap was between them. "All right, see you later, dickheads," Mancuso thought.

That hubris ended when Mancuso turned back around and tripped over one of the fences. The men started to catch up. Mancuso staggered back to his feet and started running again. He might just get away.

Mancuso, ever pushing his luck, looked behind again. A long driveway stood between him and his pursuers. I'm good, Mancuso thought.

Then from behind a house, one of the men jumped out and caught Mancuso. The group, finally, shoved their target into the car. Having caught their prize, they immediately bound Mancuso, including duct tape around his eyes. Mancuso never saw the pistol whip against his head coming.

"Do you like the taste of bleach?" one of the men asked, signaling what might be yet to come.

"Not really," Mancuso cheekily replied. The men said something about wanting a hundred million dollars. Mancuso said they had better call the guy who ran the Powerball lottery, he would pay.

The men weren't in the mood for smart remarks. The gang relentlessly beat Mancuso all the way to their destination, an industrial warehouse in another town southwest of Sydney about a half-hour drive away.

Mancuso fell silent. When faced with extreme danger, a situation where in all likelihood you know you are about to die, you may expect to try to kick and fight your way out of it. Or perhaps you might cry, beg for your attackers to stop. In his life as a criminal, that's what Mancuso had always thought he would do. But instead he clammed up. He didn't think of his parents. He didn't even think about his child. Instead, he didn't really think about much at all. He was going to die now, was his only rumination. Just a clean, empty humming of acceptance moved through his mind.

The group arrived at the warehouse at 3:30 a.m. The floor was freezing; Mancuso's bare skin slammed against it.

That was when the real beating started.

Mancuso was conscious, but the gang beat him so much he couldn't tell exactly which part of his body they were hitting. In that violent haze the men yanked out three of Mancuso's toenails. He doesn't know how the kidnappers did it, he didn't see any pliers.

As Mancuso lay on the floor after an hour of severe thrashing, his face pointed to the ceiling and "Unstoppable" tattoo speckled with blood, one of the kidnappers took out Mancuso's Anom device and snapped a photo of the damage. The kidnapper sent it to a contact stored in the phone.

"Hello brother," the message read. "Send to his friends who value his life and will negotiate."

"What do you want?" the contact replied.

"Get his manager and partners to contact us," the kidnappers wrote, seemingly referring to Mancuso's business associates in the crime world.

"OK I will get back to you shortly or have them contact you," the contact added.

"Sooner rather than later. He goes in a hole by nightfall," the kidnappers wrote.

Over Anom, the kidnappers explained they wanted thirty million worth of cash or "product"—drugs.

While Mancuso was helpless on the floor, a new thought kept running through his mind: "Fuck me, how the fuck do I get them to shoot me fucking soon so I don't have to sit on the factory unit floor so long?"

Meanwhile at the bungalow, Joe phoned the police as soon as the men left. Joe's daughter did the same when she and her boyfriend locked themselves in their room. Soon after, the police and an ambulance arrived. The paramedics wanted to take Joe to the hospital, but he didn't want to leave his family.

Joe told the local police what happened, but he couldn't help them much. All he thought was that someone had tipped off the group to Mancuso's location that evening. That was the only night Mancuso was staying at his father's bungalow.

What did help was the Anom phone the kidnappers had taken. Unbeknownst to them, the kidnappers' messages ended up right with the police. Mancuso's bloodied face flashed on a screen.

Very shortly after the initial kidnapping, a black armored vehicle pulled up outside the warehouse. Its bulletproof windshield guards made the vehicle look like it was ripped straight out of a war zone.

A police squad dressed in black body armor, balaclavas, and tan helmets piled outside the door. Many were ready with semiautomatic assault rifles. Mancuso heard them outside.

You're surrounded by a heavily armed tactical squad, the police yelled, over and over again.

The kidnappers panicked. How had the police tracked them to the warehouse so quickly? Not seeing another option, they cut Mancuso's bonds so he could leave. The group then huddled elsewhere in the building.

Mancuso walked out of the room toward the police. The rescuers seemed to treat him as one of the kidnappers. They pointed their guns directly at Mancuso and told him to put his hands up and turn around. Mancuso thought he was going to get another smack with a weapon.

"What's your name?" one of the officers asked.

"Dil-lan Man-cuso," Mancuso mumbled, not able to clearly say his own name through his injuries.

"What?" the officer asked.

“I’m Dil-lan Man-cuso!” Mancuso replied, still unable to get the message through.

There was no way Mancuso was packing a gun—his penis was visible through the thin layer of his underpants—but one of the officers searched him. After not finding anything, he directed Mancuso to the back of the crowd of the police.

When Mancuso got there, still with weapons pointed at him, another officer asked, “Are you Dillan Mancuso?”

“Yeah, I’ve been trying to tell you that,” Mancuso said. Mancuso’s smartass attitude was back.

The sun was now up as Mancuso hobbled out of the factory unit and into the fresh air. Two tactical officers directed him to a white SUV, where he used its open trunk as a makeshift bench. While Mancuso sat hunched forward, a voice blared over the police loudspeaker system in a heavy Australian accent.

“You need to come down to the ground floor door, nothing in your hands,” an officer told the kidnappers, who were still holed up inside.

Seeing no escape from the surrounding armed police, the men eventually exited the building into the car park.

As the captors stepped outside, the police ran toward them with their weapons drawn. “Get your fucking hands up,” one officer yelled. “Get on the fucking ground! Get on the ground!” The police dispersed and took down multiple members of the gang at once, with sometimes two officers per suspect. The men got down to their stomachs as the police pointed their rifles. Once tied up, the men lay helplessly on their sides on the floor. Officers then pulled the suspects by the arms and put them into holding vans. The alleged gang, it turned out, was a ragtag group of mostly twenty-somethings, and even one teenage boy (several are still awaiting trial). Authorities allege that in an attempt to destroy physical evidence, the men started a fire. A fire engine then blasted water through a broken window of the building’s upper story to put out the blaze.

A supreme irony ran through the entire kidnapping and rescue: As someone who sold encrypted phones, Mancuso helped people avoid law enforcement surveillance. Now that same type of spying had let the police track down his captors. Anom had saved his life.

Looking back later, Mancuso believed the reason his bail conditions banned the use of Ciphr was to encourage him to move to Anom. Because the phone was broken for a while, he didn't use it to plan any crimes. His first piece of Mancuso Luck. And then another dose when the Anom phone led police to his captors.

The police told Mancuso they believed whoever ordered the kidnapping would try again. They indicated in conversation with Mancuso the mastermind was someone overseas. Mancuso later asked a judge to revoke his bail and put him back behind bars until his sentencing the following year. Inside, Mancuso was placed in solitary confinement for his own safety. The constant lack of human interaction ground on his mental health.

"I am advised that you are at serious risk from members of the Comancheros, Lone Wolves and Mongols Outlaw Motorcycle Club Gangs (OMCG)," a letter written by the prison to Mancuso read. "Due to the risks involved, it would be unsafe to place you within [the] mainstream population."

"I empathise with your mental health concerns," the letter concluded, and recommended he get counseling available in the prison.

But at the moment when he was rescued, Mancuso was safe. The authorities might not continue to be so lucky. As Anom reached a breaking point, the next Mancuso could fall through the cracks. It was time for Anom's finale.

Chapter 31

Dominoes

The plan was to follow the sun. Australian authorities would start their arrests at night, followed by more during the day. European police in Sweden, Germany, the Netherlands, and other members of the task force would then follow suit and conduct theirs in the early morning, local time, hopefully catching their targets while they lay in bed.

Shortly after, Australia would be the first to publicly announce the operation in a press conference. Then, as the sun traveled west, a conglomerate of officials would host their own press conference in Europol, flexing their successes. Finally, after the sun rose over the horizon in San Diego, US authorities would broadcast the final announcement and take responsibility for running Anom. All the while, FBI analysts would continue their constant monitoring of Anom chatter in case of an emergency.

The twenty-four hours beginning on June 7, 2021, were going to be a nonstop, intercontinental line of dominoes. Ten thousand police around the world would act that day, in what would be the single largest law enforcement action in history.

The raids in Australia had begun early. Authorities had been making arrests through April and May, and never quite stopped. On June 6, the night before other agencies would strike, a combined AFP and NSW team hurried to its target. In one of the first raids, a black police SUV rushed up the driveway of a suspected Comanchero associate's house. Officers banged repeatedly on the door, and the police hurried in.

With a loud crack of wood as the door came off its hinges, the line of dominoes started to fall. Over the coming hours and into the day, the AFP and state police swept across the entire country. SWAT teams climbed ladders into high-rise apartments. An officer cut through a glass patio door to let their team inside. Suspects were cable-tied and parked on the side of their beds. The police seized sports cars, Harley Davidson motorbikes, bundles of cash.

Questions, naturally, started to rise. What evidence did the police have against the alleged drug traffickers, weapons smugglers, or money launderers grabbed by the AFP and Australian state police?

Ayik, with his deep Comanchero connections, had some insight. He sent a copy of a search warrant he obtained to an Anom worker. The warrant included the target's alleged Anom username and the unique serial number of their device, information the police should not have unless someone, or something, had fed them the data beforehand. As the raids pressed on, the Anom worker's phone lit up with messages, and they started to put two and two together: these raids were connected to Anom.

As suspicion mounted inside Anom itself, Afgoo had to fend off his own employees. If they figured out Anom's secret at the last minute they might warn users in Europe. Afgoo ordered one worker to turn off their Anom phone. Afgoo said that he would handle any inquiries from customers about what was happening.

As Australia reached late morning on June 7, on the other side of the world it was two a.m. for Börjesson, the Swedish detective who investigated the Firm. That night he walked into a secure room in the Örebro, Sweden, police station. The detective was accompanied by two other people, an intelligence coordinator and the head of the SWAT teams. An oval table sat in the center, with office chairs and computer docking stations for each of them. Communications equipment let the three speak with officers in the field. Börjesson jokingly compared the environment to the Situation Room in the White House, where US presidents oversaw dramatic raids and missions. Only this command center was in a small Swedish city across the road from a burger joint.

It was going to be a long night and morning for the team. They planned to take down targets in three locations around Stockholm simultaneously: an apartment where Jovanovic, a member of the Firm, lived with his partner

in the north of the city; another in the suburbs where Bogebrink, the Firm's dark web expert and accountant, lived; and then the Anom satellite office in an industrial estate to the south. At the time of the amphetamine lab raid in December 2020, the Swedish authorities had deliberately let Jovanovic and Bogebrink be, to gauge their reaction to the seizure and see if they made any more mistakes. Since then, Börjesson and his team had built even denser cases against the Firm, documenting the crimes they went on to next.

Cups of coffee in hand, Börjesson and the two other officers rigged up their equipment and took their seats at the table. The group first checked the latest surveillance footage to make sure their targets were where the police expected. Then as the late night morphed into the predawn morning, the SWAT teams quietly headed out. Through radios the three officers at the table spoke to the teams on the ground: they were in transit, getting closer to the objectives. The officers at the table didn't have a live visual feed of what the teams saw; the audio from the radios would have to do.

The SWAT teams needed to strike each target at high speed and at the same time. That way, Bogebrink or Jovanovic wouldn't have a chance to wipe their computers or destroy any other evidence. The Firm's members were technically sophisticated and may have set up kill switches that could erase their devices if they realized what was happening. Even though the authorities had the Firm's Anom messages, to successfully convict someone in court they needed to gather all the evidence they could. The Anom texts were certainly incriminating, but potentially not enough to put someone behind bars, depending on the crime.

Börjesson's team especially had to prove who owned each Anom phone. For weeks the team had done a lot of this work in preparation for the big day. They conducted physical reconnaissance to match what was said in the texts to real-world actions. Investigators obtained other electronic evidence to corroborate what a target had been up to. Once inside the apartments, the police would likely find additional evidence, including the Anom phones themselves.

"We have to have some reality. We have to make sure that the things written in the chats are the same as in real life," Börjesson said.

There was an even more important reason for the strikes to hit at the same time. They were just one part in that global line of dominoes. If Börjesson's team messed up, maybe the Firm would warn other Anom users

about their impending doom. The team did not know if the Firm had some sort of alarm line set up, where it could alert other members or organizations of a raid in progress. If the team didn't strike perfectly, their domino might stand rigid, or fall in the wrong direction, ruining other operations too. Börjesson and the intelligence coordinator knew this raid was bigger than three Swedish officers in a regional police station. The success not only of his own investigation weighed on Börjesson's shoulders but that of everyone else's as well.

"We can fuck it up for a lot of people," Börjesson said.

The SWAT coordinator at the table, meanwhile, was blissfully in the dark. All they knew was what doors to tell their team to kick down. They had no idea that the FBI ran Anom or that this raid was one of many.

At just before six a.m., the SWAT teams were in position.

We are at the point of no return, the SWAT coordinator said to those around the table. Was the mission a go or an abort?

Worries flashed through Börjesson's mind. What if someone gets hurt? Have we prepared as much as we could? There was no more room for more surveillance, no more double checking, no scrolling through collected intelligence. They couldn't tweak the position of their domino any longer.

Nothing was left to do for Börjesson but to sit back and listen to the raid through the radios. Whatever happened next was out of his control.

"Go," came the order from Börjesson, still nervous about whether he'd missed something.

At first, there was silence. The officers around the table looked at one another. Then, a cacophony of action: The crack of a broken-down door. A plant pot being smashed. Men shouting. A scared dog running away from one of the homes. SWAT teams shouting orders at the suspects. A panicked partner of a target. For a minute and a half, Börjesson held his breath in anticipation and listened.

One by one, the SWAT teams reported their status. Target arrested. Area secured.

Börjesson felt a rush of relief. Nothing had gone wrong. No one had been hurt. The Firm was no more, and Börjesson could breathe again.

After the stress subsided, Börjesson's group reported the Firm arrests up the chain of command to Stockholm. On a whiteboard, the Swedish National Police listed sixty-five targets in the country. As the reports from

regional forces like Börjesson's came in, officers made a mark next to each target to record their arrest.

At around the same time, Cheviron, Stevens, and Bobbitt watched the moment Dutch police executed their raids from a command center in the Netherlands. On the wall were screens of drone, helicopter, and body cam footage. The FBI agents sat at the back of the room dressed in their suits, all three anxious for what was about to happen next.

Kraag, the senior cop in the Netherlands, was much more relaxed. He walked in and out of an equivalent room inside Politie's headquarters. Smile on face and coffee in hand, he reveled in the moment as staff took their positions. By now, he had done this a couple times before with Encrochat and Sky. Enjoy the moment, Kraag told the operatives in the room. It is rare for the police to be in front of the game.

Kraag may have been calm, but he didn't have countless possibilities eating at his conscience. He was responsible for his Dutch police officers and their targets. Yes, if something went wrong that might have some knock-on effects. But the FBI agents, meanwhile, were ultimately responsible for each and every agency that used the Anom data. The Dutch, the Germans, the Swedes, every member of the sixteen-strong task force.

The number of officers on the ground was an unprecedented amount of nearly simultaneous activity, with huge space for something to go wrong. Bobbitt thought about the fact those police officers were going to blow the doors off hundreds of the worst criminals in the world. What have we missed? What have we mismanaged? What if someone gets shot?

Bobbitt felt that pressure mount but didn't want to say so out loud. The other agents kept their bubbling thoughts to themselves too. The stress building, Cheviron started to laugh, anxiously. Dutch officers turned around and gave the noisy FBI agents a dirty look.

There wasn't anything for the agents to do but watch the dominoes fall.

In Politie's headquarters, a large operation status board displayed a checklist of targets. At the start, all of the targets were marked as red. Orange would signify a raid in progress, and then green for a successful arrest. Everything switched from red to green.

These moments were microcosms of what was happening in dozens of regional and federal law enforcement agencies across the world at nearly the same time. Next, each country communicated their successes to

Europol, the nerve center that brought information from the national police forces together and where the FBI agents headed after watching the Dutch raids start.

From all across the planet, news of the arrests piped through to Europol's headquarters, where officers sat behind screens and ticked off the names of high-value targets on their own whiteboard. Excitement filled the air—weeks and months of work reading text messages now became real for many of the people there.

Officials inside Europol couldn't kick back and watch the fireworks, though. They kept up a constant ping-pong rally of information between different countries to locate, chase, and arrest certain targets outside of their own borders.

At around midday, one of Sweden's regional units phoned Urve, the country's person inside Europol, with bad news. The unit had a GPS tracker on a target's car. He was suspected of, among other things, kidnapping and extortion. But after seemingly realizing a wave of arrests was washing over the country, he had escaped from Sweden. Driving south at two hundred kilometers per hour, the suspect was now in Germany.

Urve, who had been drinking coffee and Coca-Cola to keep going, ran from her office in Europol to her German counterpart, a tall man with long hair. Urve said she was working on getting the arrest warrant for this target into Europol's system. The German official contacted operational units in his own country and had a team follow the target.

A short while later, the German representative came back. He now had a mobile phone to each ear. "Scheiße!" he shouted into the phones. In one side was the German team. In the other was a Dutch team. The suspect had continued driving and was now in the Netherlands. Even during the high-stakes moment of tracking down a violent criminal, Urve couldn't help but laugh at the sight of a six-foot-five man juggling multiple phones.

Should we arrest the suspect? the German representative asked. Yes, we have the arrest warrant, Urve promised. It just still hadn't appeared in the international system yet. The German official gave the order and a team grabbed the Swedish suspect.

The targets were so voluminous throughout the day that one country reached its capacity for arrest warrants. Sweden, Finland, and the

Netherlands sent so many requests to Spain for arrests that authorities ran out of personnel to be present at all of the house searches, Urve said.

Just as organized criminal networks now operated without borders, the officers inside Europol did the same. They instantaneously collaborated, their own borders practically meaningless.

Chapter 32

Reveal

On the ground, Anom's users were in a panicked frenzy. Christof, now one of Anom's main sellers, slowly woke up from a night out to a barrage of messages.

"Wipe the phone. Wipe the phone," one said.

In his coastal penthouse bedroom, Christof picked up his laptop and opened it to log in to the Anom portal. Here, he could push the command to his clients' phones that would delete the data stored on them, something he had done countless times before. But he couldn't log in. The site would not load. Christof tried phoning some contacts to find out what was happening, but they didn't pick up.

Christof had been right when he told his wife something big was coming. Now in the short time from first waking up to seeing that he was locked out of the Anom portal, there were already too many signs to ignore: this was it. Christof told his wife this was the day.

Just minutes after Christof first checked his Anom messages, the doorbell to his penthouse rang. Over the intercom, a man said they had crashed into Christof's motorcycle; please could he come downstairs?

After the repeated bouts of surveillance on him, his clients, and other Anom sellers, this must be the cops, Christof told his wife. There was no point fighting. Christof powered down his laptop, grabbed his wallet and some extra cash, and made his way downstairs.

At street level two men stood next to Christof's motorcycle. One of them slyly flashed a police badge from his pocket. Christof didn't want to speak to the men in front of his neighbors so he agreed to go with the

officers to the local police station. Once all three were in an unmarked police car, the officers revealed why they had visited: Christof was under arrest due to an extradition request from the US.

"What the fuck, are you sure you have the right guy?" Christof asked. He hadn't done any business in the US—he told the officers as much. Why would the US authorities have any interest in him? Sitting in the backseat as the police drove to the local station, Christof thought this must be about the recent Sky shutdown a few months earlier. Perhaps the authorities were now targeting the vendors of the phones.

It wasn't until a day later that Christof learned what this was really about. Christof joined his initial court appearance via video link. During that hearing, a local prosecutor read the charges: money laundering, drug trafficking. Then they mentioned "Anom."

This was impossible, Christof thought. Christof told his clients it was highly unlikely Anom was compromised because it had been around a much shorter time than companies like Sky or Encrochat. Questions rushed through Christof's mind: Did the police have the content of Anom messages? Was this arrest for things he had allegedly done, or more the behavior of his clients? It was, as he would soon find out, very much the former.

"What the fuck," Christof thought.

That sentiment spread across Anom's entire user base when acting US Attorney Randy Grossman walked up to a podium inside the US Attorney's Office in San Diego. In a press conference room on the sixth floor, emblems of various US law enforcement agencies hung on the walls. Journalists sat in lines of chairs. The largest law enforcement operation in history had started in a crummy office downtown, and this was where it now ended.

On a small stage with blue drapes, Grossman spoke into a microphone and pulled the curtain back on Anom: it had secretly been run by the FBI.

"For the first time, the FBI developed and operated its own hardened encrypted device company, called Anom," Grossman told the audience of

reporters and law enforcement officials, as well as people watching the livestream. In its own earlier press conference the AFP had mentioned running Anom but not provided many specifics. Europol did much the same. Now Grossman, and by extension the US government, showed the world how the FBI had masterminded Anom for years.

A map of the world appeared on a large screen to Grossman's right, with colored-in countries showing where Anom phones had been. The majority of the map was awash with orange—more than a hundred countries in all. The screen then displayed examples of Anom messages, photos, and subsequent drug seizures. Anom's users were completely naked and on blast to the planet.

"Operation Trojan Shield has shattered any confidence criminals may have through the use of hardened, encrypted devices," Grossman said. By using Anom, "the criminals were not underneath the radar, they were on it," he added.

Young was back too, albeit this time in the audience and not in front of it. During Anom, his beard had turned from brown to gray, but maybe that was more to do with his kids than the massive wiretap. Standing at the back of the room watching Grossman speak, Young couldn't help but feel ambivalent. On one hand, he was proud of his colleagues and the operation that he initially spearheaded. Especially Meghan Heesch, one of the prosecutors he handed over the Anom reins to when he left. The underdogs from San Diego had, somehow, pulled it off. On the other, Young had a lingering feeling Anom could have been even bigger and better. If colleagues had gone along with his plan to intercept messages inside the country, Grossman might be announcing the arrest of five hundred people inside the United States that day as well.

Young had watched the AFP press conference from his office, in which the Australian prime minister, the leader of the country, spoke. The US did not push the same weight behind their own announcement. He saw an amazing juxtaposition between Australia, which put everything into this and got phenomenal results, versus what the United States did. The stage was in San Diego, not Washington, DC. And in Young's eyes, the operation was being finished off by people who weren't ever supportive of it in the first place.

The Department of Justice may not have even announced its running of Anom at all if not for some of the officials involved. Bobbitt recalled the Attorney General's Office repeatedly delayed any confirmation of what the press response, if any, would be. Eventually, Bobbitt says he told a staff member of the Attorney General that I am going to write our press release. I'm going to tell you what it should be. You can make whatever changes to it you want. If we don't hear back from you, that's what we're giving to Europol and our partners. We're moving forward. We cannot and we will not wait.

From the stage Grossman then provided a final cadence. He elaborated on the unsealing of an indictment against Anom's most prolific sellers. These Anom distributors unknowingly did the FBI's dirty work by getting the phones into customers' hands. And now, in an ironic twist of the knife, the US was charging them with RICO Act charges too, for allegedly selling the phones knowingly to criminals, and issuing wipe commands when phones had been seized. The indictment named Ayik, Catanzariti, Microsoft, Wijzijn, Bobby, Christof, and eleven others. Like Christof, eight of those were detained during the wave of arrests. The rest were fugitives.

Microsoft was one of the fugitives now indicted by the DOJ. In the wake of the FBI's startling admission that it ran Anom, Microsoft finally knew the cause of all his misfortune over the past year. The drug lab shutdown, the tracking of his cocaine shipments—it was the FBI and Anom all along.

Microsoft thought he was going to be part of Anom's meteoric rise to the top of the encrypted phone industry. Instead, many people were now going to sit behind bars because he insisted they switch to Anom. The green icon next to his profile picture in the Anom app, which showed he was online, vanished. Phone numbers he used for WhatsApp and Signal went offline. Microsoft went dark.

Shortly after the action day, Athit, one of the Anom developers, lay on his bed in Asia with his MacBook on his chest and visited the company's website. The screen flashed a bright white light as it displayed a new message on the site: "This Domain Has Been Seized," it read, followed by the emblems of the FBI, Operation Trojan Shield, Operation Ironside, and the AFP.

Below those coats of arms was a red box with white text. "Law enforcement has been monitoring messages and attachments from the

ANØM platform. A number of investigations have been initiated and are ongoing," the box read. Just like with the earlier seizure notice on Phantom Secure, the site included a form where Anom users could submit their personal details to, allegedly, learn whether they had been swept up in the operation. From the outside, there was no telling what authorities might do with that data.

As he scrolled through the vandalized Anom site, Athit was shocked. He had worked on Anom for years and never suspected it was secretly run by the FBI. Still in bed, he called for his wife and showed her the seizure notice.

While the dust settled around Anom's explosion, Afgoo sent an internal email to his developers to come clean with them.

"I regret to inform you that Anøm is closing operations permanently," it started. "If you follow the news, you may be aware that Anøm shuttered service on June 7th 2021. Prior to this, I was not authorized to inform the team of Anøm's true agenda—to legally infiltrate the communications of organized crime.

"To this end, Anøm has achieved phenomenal success. I feel proud to have worked with you and what we have achieved together. Anøm saved lives (literally) and made the world a safer place," Afgoo continued.

After the raids, Cheviron, Stevens, and Bobbitt headed out to the patio once again for their post-takedown gin and tonics. Finally, they could relax. But barely after the first round was poured, Stevens got a call on her phone. It was a contact from Austria. The officer didn't call to congratulate the agents: he had a problem.

The Austrian contact said a user had sent a certain video across the platform. Gangsters had someone in a hole, were torturing him, urinating on him, had broken his fingers, and were discussing plans to beat the person to death with a hammer.

Stevens did what the agents had done dozens upon dozens of times before and opened her laptop to pull together intel on where this person might be. Anom's no longer secret surveillance provided solid information. She sent what she found to a legal attaché office, who handed the information off to local authorities to hopefully save this person's life. Given the non-friendly relationship the FBI held with the country, it was unlikely they would find out what happened to the victim.

The reality was, with Anom winding down, that intelligence would soon dry up. The FBI would no longer be able to provide tip-offs that someone was in danger and needed help. I wish I could have done more, Stevens told the other agents around the garden table. Bobbitt pushed back and listed off some of the successes Anom led to.

"There's absolutely not more you could do," Bobbitt said.

The agents returned to their gin and tonics.

Epilogue

The hotel was entirely overrun with cops. Cops in suits. Cops in more casual clothes. Cops eating the buffet of sliders and shrimp. Cops helping themselves to the unlimited coffee. And cops joking and laughing while presenters spoke from the stage in a large conference room.

At the two-and-a-half-day law enforcement and industry-only summit in Vancouver, Canada, in April 2022, the attending officers milled between the room for presentations and a market-style area with contractors trying to sell their wares. From small desks covered in brochures, the vendors offered different ways to track, subdue, and interrogate targets.

After a long first day of seminars about artificial intelligence and cybersecurity, it was the FBI's Muse and Kalina's turn to speak. At just past 3:15 p.m., the pair walked onstage and overlooked the audience, packed around circular tables. The pair were here to talk all about Operation Trojan Shield, nearly ten months after the FBI revealed it had run Anom for nearly its entire existence.

Kalina opened with a joke. After landing and passing through the border, Canadian immigration were "so nice." Then they got into a cab. The driver was "so nice." Then at the first talk of the conference that morning, Beverly Priestman, a gold medalist and head of the Canada Women's National Soccer Team, spoke about beating the Americans.

"Wait a minute, this has taken a bit of a turn," Kalina said to laughter from the audience.

For the next nearly hour and a half, Muse and Kalina gave the attending law enforcement officers a high-level run-through of Anom. As the pair's voices boomed through the hall, participants at one table flicked through details of the case on their phones. They Googled news articles and giddily showed each other photos of the Anom app they found online.

Muse and Kalina reeled off Anom's seizure and arrest figures: 500 arrests on the joint action day; 12 tons of cocaine; 1.5 tons of meth; 1.5 tons of amphetamine (such as Microsoft's lab in the countryside); 17 tons of precursor chemicals; 22 tons of hash or marijuana; 300 firearms. The seizures had continued well past Anom's big day of action the previous year. In September 2021, UK authorities intercepted a luxury yacht called the *Kahu* sailing from the Caribbean. While at sea, police raided the yacht. Packed among the yacht's interior was a massive two tons of cocaine. The tip came from the AFP's earlier monitoring of Anom.

Anom's arrests had also increased since the joint action day. At the conference Muse told the audience, "We did surpass the one-thousand-arrest mark a couple of months back." It was difficult for the San Diego FBI to keep tabs on how many people each agency involved in Anom had arrested. But the number is likely to keep climbing. Since the joint action day, the San Diego FBI has received requests from even more countries for data that might help them in their own investigations. The data has been used in courts to successfully prosecute and convict people, not just seize their drug shipments. And with Anom's secret now revealed and much less worry about corrupt officials leaking it, the FBI traveled to other countries outside of the OTF and provided them with information. That includes Serbia, where the FBI's Belgrade office is also responsible for liaising with Bosnia-Herzegovina and Montenegro. For these trips, the FBI tried to prioritize countries where Anom saw the most users—an indication of Anom's growth in the region.

Some of the more recent arrests were in Australia, where authorities entered a second phase of Operation Ironside in December 2021. This new wave of action identified around 160 targets, including trusted insiders, perhaps at ports or logistics firms, who help facilitate drug shipments, and Italian organized crime figures based in Australia. Later, the AFP secured more top priority targets thanks to Anom. In August 2022, Australian police got their hands on Mark Buddle, the leader of the Comanchero biker gang, and part of Ayik's Aussie Cartel. Authorities say Buddle was allegedly connected to a drug trafficking syndicate that operated out of Hong Kong and Turkey and that used Anom. Shortly before news of Anom broke, he left his hideout in Dubai and went on the run in Iraq, before returning to Northern Cyprus. Turkish authorities caught Buddle and deported him to

Australia. The Australians officially had the head of the Comancheros in their hands. The arrest, like Operation Ironside more generally, left the Comancheros in tatters. Duax "Dax" Ngakuru, Ayik's childhood friend also hiding out in Turkey, was then said to have become the international leader of the biker gang.

But barely five months later, Turkish authorities busted him too. As soon as the Comancheros spawned one head to replace its severed one, authorities sliced it off again. At the time of this writing, it appears the leadership of the Comancheros is in flux. With those arrests and a handful of others, Turkey became more hostile to its criminal residents, just like Dubai did.

Ayik appeared immune to arrest even as his associates dropped off one by one around him. Six months after the joint action day, once criminals learned he was, in a way, the reason they had been spied on through Anom, a dormant Google account in Ayik's name sprang back to life. Its owner left reviews for restaurants and tourist hot spots all across Turkey. Despite the AFP's insistence, or hope, that Ayik turn himself in, he did not.

Microsoft too seemed safe in Turkey. In June 2023 the US State Department offered a bounty of up to $5 million for information that led to his arrest and/or conviction. That was an extraordinary amount of money: the State Department offered an identical sum for each of the four sons of infamous drug kingpin El Chapo, as well as the boss himself at one point. The key to Ayik's and Microsoft's freedom was that both had obtained Turkish citizenship, creating an impenetrable legal barrier around them.

Members of the underworld were in shock then when Turkish authorities did finally strike against the pair. In a series of dramatic raids later that year, police grabbed Ayik, Microsoft, and more than thirty other people, including "The Turkish Boys" Baris Tukel and Erkan Yusef Dogan. In a video, Ayik laid on his stomach while being detained. Propped up to his knees, Ayik stared forward into space, shirtless. The king of encryption was finally in handcuffs. Microsoft looked gormless when heavily armed officers surrounded him.

Behind the scenes, the AFP had worked with their Turkish counterparts on a compromise: prosecute Ayik under Turkish domestic law rather than extradite him to Australia for crimes back home. That way, even though Ayik was a Turkish citizen local police could still disrupt his drug

trafficking empire. Ayik's direct workmates didn't think this was the conclusion of the kingpin's story though. Maybe he will slip out of the authorities' hands once again. "It's a big blow but it's not the end," one said.

In the months and year following Anom's big bang, authorities continued to pick up other alleged Anom phone sellers. Those included Shane Ngakuru, whom Thai police grabbed just south of Bangkok in October 2022. Ngakuru was a member of the Comancheros and Dax's cousin. Anom struck the outlaw motorcycle gang, again.

The Belgian police may have only arrested around two dozen people when it first announced the Sky hack. But that access to hundreds of millions of messages led to many, many more. In November 2022, Europol along with police in Belgium, France, the Netherlands, Spain, and the UAE targeted a so-called super cartel and arrested forty-nine people in part using Sky messages. In May 2023, Europol announced the takedown of the Balkans' biggest drug lords. What the encrypted phone cases managed to do, and continued to do even years after the fact, was bring down groups that were ordinarily resilient, or even invisible, to the authorities.

The hack of Encrochat continued to provide results too. In 2022, cops chased down a most wanted fugitive who was hiding out in Marbella from UK police.

Zooming out and looking at the Encrochat, Sky, and Anom investigations as one overarching campaign, nothing quite like this grand master plan has ever struck organized crime before or since. While Anom was the biggest single day of law enforcement action, Sky and Encrochat provided more intelligence, and arrests, after the fact. Europol's most recent figures put the number of related arrests across all three operations at more than ten thousand people. It's as if law enforcement did arrest the equivalent of Phantom Secure's entire user base. Only in the end, it was across three companies and a worldwide set of agencies. (That figure may now be higher; in June 2023 authorities announced the Encrochat operation eventually led to more than sixty-five hundred arrests by itself.)

Europol puts the total number of seizures at more than two hundred tons of drugs and more than €700 million ($761 million) in cash. That's not including other types of assets, be those luxury vehicles or anything else. For context, individual investigations into criminal groups sometimes net

hundreds of kilos of drugs or a few million in cash. This penetration of the encrypted phone industry multiplied that by something like a thousand.

After the hack of Encrochat, the gathering of Sky messages, and the puppet-mastering of Anom, multiple agencies see these large-scale, bulk interception missions as the future of law enforcement's fight against organized crime.

"It's not that I hope; I know that there's going to be more investigations" like these, Kraag from Politie said. In February 2023, Politie announced it had infiltrated another smaller encrypted phone firm called Exclu and read users' texts.

Perhaps more important than the constant churn of new organized crime leaders and recruits were the drug trafficking industry's techniques: its secrets of how to package cocaine and smuggle it across borders, or the sort of people it flipped inside ports or businesses. That information was arguably more valuable to law enforcement than shutting down any one syndicate. And now many of those secrets were burned.

Europol's Liukkku said the data from Encrochat, Sky, and Anom provided great insight into how organized crime worked. But, just a year or two later, that information was already out of date, he said. Criminal networks evolve and are highly resilient.

In November 2022, the Swedish detective Börjesson, who took down Microsoft's drug lab, was still up to his neck in investigations spurred by the Sky and Anom operations. "There's still a lot of work to do. It's a gold mine," he said.

But the investigations were not silver bullets. Whereas the number of shootings in Sweden went down after the Encrochat hack of 2020, two years later the violence skyrocketed back up. Sweden hit a new record for fatal shootings in 2022.

"It's worse than ever," Börjesson said. Combating organized crime is a lot more complicated than arresting as many people as possible. Shootings

are the way young criminals solve their issues among one another, Börjesson said. “I don’t know how to stop it. It’s not good.”

Urve added, “I actually thought that it would change in Sweden” after arresting so many high-level criminals who used Encrochat and Anom, acknowledging that she may have been too blue-eyed. “Maybe it also left a vacuum, because the number of criminals ready to take the[ir] place is so big.”

Anom did not save Sascha, the man murdered on the bridge in Stockholm. Using Anom messages after the fact, though, Swedish police identified the killers and a court convicted three men for their role in Sascha’s assassination. Two received life sentences for murder, and the third was sentenced to fourteen years in prison for incitement to murder. An appeals court upheld the verdict.

Arguably, that prosecution may not have happened if the hit was planned on another encrypted chat platform that the authorities did not have access to. Said Sadat, a man Swedish authorities are pursuing in connection with Sascha’s murder and who Microsoft hired for other hits, was eventually found in an Airbnb in Lebanon.

During their Vancouver talk, Kalina and Muse didn’t mention Sascha’s murder. Kalina did say, “I think in Sweden alone they’ve solved close to a dozen murders from the information from Trojan Shield.”

Anom’s impact on solving those murders is clear, but it may have only provided a slight dent into the overall drug trade. Antwerp continues on its path as a city increasingly governed by the shadow economy. In January 2023, an eleven-year-old girl was shot dead. She was living in a house that was linked to drug-related activities, authorities said. The next day, authorities coincidentally announced that cocaine seizures in the port had reached an unprecedented new height, with over one hundred tons in 2022. Many of the previous seizures could be attributed to the Sky or Anom operations. But the numbers kept increasing even after those operations were done and dusted. That meant, most likely, police were once again only seeing a tiny sliver of the true number of narcotics that came through the port. The drugs just kept coming.

“Despite unprecedented levels of law enforcement cooperation and operational success based in part on intelligence from encrypted communications investigations, the cocaine market appears to have

remained remarkably resilient, reflected in high purities and stable prices at retail level," Andrew Cunningham, head of drug markets and crime at the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), told a journalist in June 2022.

As sizable as the seizures were for law enforcement, they were paltry for organized crime overall. Other shipments have already been waved through. Other players have already taken the place of those arrested.

"It doesn't matter if you take the containers with [a] thousand kilos of cocaine. They keep sending it," Urve added. "Maybe we should stop counting the numbers and the kilograms and instead look [at] what effect did this action have? Did we actually arrest the right people?"

What the Anom and related operations have ushered in is an entirely new way of investigating organized crime. One that brings up questions of privacy, proportionality, technology, and legality, with very little to no discussion of whether law enforcement agencies should carry out these types of bulk interception operations.

In the UK, a long-running legal dispute argued whether the messages could even be used to prosecute defendants. It boiled down to whether, in a highly technical sense, the messages were collected through interception or hacking. In a quirk of UK law, intercepted material is largely limited to intelligence purposes and not evidence before a court. Those debates are ongoing.

Defense lawyers have vigorously pushed back at the intense secrecy shrouding certain parts of the operations. Lawyers working on Encrochat-related cases published an open letter saying their clients were not receiving fair trials, in part because French authorities refused to explain how the messages were harvested.

"It is clear that law enforcement agencies in each of our countries should have the tools required to investigate serious organised crime, such as the type revealed by the EncroChat hack (with the use of sophisticated methods, in cooperation with agencies of fellow EU Member States and other international partners). However, investigative tools have serious implications on people's fundamental rights, and they must therefore be rightly framed in law, with adequate procedures and safeguards," the letter read. The French Constitutional Court went on to rule that the secrecy around the case is constitutional.

In October 2022, the Italian Supreme Court publicly said prosecutors should provide more information on how exactly they harvested Sky's messages. Then in November, a Berlin court sent a request to the Court of Justice of the European Union to verify whether the sharing of data from Encrochat complies with the European Union's laws. And with Anom, the FBI has refused to reveal the name of the third country that funneled Anom messages on its behalf, meaning defense teams have not been able to verify themselves that collection was performed legally (the government's refusal is despite the identity of the country—Lithuania—being published in a media report in September 2023). A group of defendants in Australia joined forces to push back against the legal basis for the Anom operation. In April 2023, a judge found the police ran the operation legally.

Raza, the defense attorney who used Encrochat and Sky phones, later found Dutch authorities had continued to read his messages with his clients despite this not being allowed. Raza was not the only lawyer who had his messages read, and he went to the Dutch media to raise the alarm about the overstepping.

"I didn't do anything wrong," he said. Yet, the authorities read his chats. Raza said the authorities later apologized to him.

Ramos, the convicted CEO of Phantom Secure, is due to be released from a US prison in November 2024. The RCMP identified the person who leaked to Ramos sensitive information: Cameron Ortis, a top-level RCMP official. Authorities charged him with violating Canada's Security of Information Act. He was found guilty in 2023.

Eap, the CEO of Sky, continues to maintain his innocence and remains free in Canada. In November 2021, lawyers working for Eap said they were going to fight the US government to regain control of Sky's web domains. Ashwin Ram, one of those lawyers, said that Sky and Phantom Secure were fundamentally different companies.

"While Phantom operated in the dark and wiped devices held by law enforcement, Sky had a public website and platform, and created policies to prevent that from happening and had an actual track record of refusing to wipe devices that were known to be under investigation. More fundamentally, Sky took steps to root out bad actors, and when Sky became aware of illegal activity, it terminated the source of that activity. Phantom did the opposite," he wrote in a statement at the time.

Sky's lawyers maintain that Sky was collateral in the authorities' investigation of the encrypted phone industry. By their read, Sky was a sacrificial lamb, killed to lure users over to Anom, which the FBI controlled. A legitimate company that was shut down to help Anom grow.

The prosecution of Eap remains on ice, until authorities manage to pull him into a US courtroom.

Other claims of being unwillingly used came from inside Anom itself. At least one Anom worker involved in the project felt like an afterthought in the FBI's mission. Used and tossed aside, with dangerous criminals now potentially thinking the workers had a helping hand in catching them.

"To the FBI we are collateral damage, they [do] not give a fuck what happens," they later recalled. "We all get nothing except wondering what might happen." Afgoo's email reminded the developers that they had signed nondisclosure agreements and that they should not speak to the media or reveal their involvement in the project publicly. For some workers, that left a years-long gap in their employment history that they would somehow need to wash over in the search of a new job.

"We wanted to make it be known that they should not trust hardened devices," Kalina told the crowd in Vancouver, referring to organized criminals. "We want them to think that, just maybe, law enforcement is listening." After that, perhaps syndicates would bail from the encrypted phone industry altogether and "get back to traditional methods, which for us is a lot easier to follow than these hardened encrypted devices."

The FBI certainly succeeded at sowing distrust across the encrypted phone ecosystem. After Anom, the underground trade of these phones became a hive of paranoia. One seller based in Europe thought it was "impossible" to rebuild a customer base with an encrypted phone now. Users just wouldn't be able to shake the feeling that the FBI might be behind whatever new device hit the market. Some users did pivot to newer, and smaller, providers, but no companies quite the size of Encrochat or Sky

exist anymore. Authorities later arrested eight people suspected of being behind Encrochat, too.

Once the public learned of Operation Trojan Shield, one of the last established players in the encrypted phone industry closed up shop. First Ciphr pulled out of Australia, where it had become the phone of choice for organized crime. Then the following year, in August 2022, it ceased operations entirely. Ciphr never publicly commented on the reasons why.

Inside the company, bosses were nervous. A Ciphr worker said management took an unannounced vacation after Anom's big reveal and seemed very agitated at the time. Several people in the Ciphr office were also aware of what happened to Sky, with the US government seizing its domains. Trojan Shield and the broader attack on the encrypted phone industry showed the extreme measures law enforcement was willing to go to, and Ciphr was a natural next target.

Some former encrypted phone users went back to old-school tactics. Rather than trust any specific encrypted device company, they bought a normal phone, took the camera and microphone out, and then threw the device away every month.

Others decided to concentrate their communications on publicly accessible secure messaging apps, like Signal.

That raises a key question: What will authorities do if their targets increasingly flock to the same sort of encrypted chat tools that everyone else uses?

The San Diego FBI said it would only look to address the specifically criminal use of any of those applications. At the same time, its position is communications that are facilitating criminal activity should never be out of the reach of law enforcement.

"I worry. I worry a lot," Matthew Green, an American cryptographer and associate professor at Johns Hopkins University, said. Green has been a fixture in the debate over law enforcement and encryption for decades. Green also worked on Zcash, a more recent form of cryptocurrency that promises to be much more resilient to tracking than Bitcoin.

He had no problem with the FBI investigating networks that were run by criminals. If anything, he was glad to see those networks get compromised.

But it is what happens next that Green is concerned about. When criminals inevitably realize that using home-brewed networks designed for

crooks is a bad idea, many will switch to mainstream products. When criminals do move to those networks, the police won't simply stop investigating. "I don't think they'll just give up," Green said.

Green brought up the example of an imaginary network that had two types of users. One-half were engaged in lower-level crime, such as sharing copyrighted song lyrics. The other half were more serious criminals. Would that network be a legitimate target in the eyes of the authorities?

"Is it 50/50? Is it 90/10?" Green asked. "I don't know where that cut-off is."

If the future of the cat-and-mouse game between law enforcement and criminals is the continued targeting of obscure phone companies, that would be less of an issue to the general public.

"However, I just don't think it's a stable future, and I think eventually we're going to run into a problem where the networks don't only have criminals on them," Green said. "That future, which I think is coming soon, is what scares me."

During the reigns of Encrochat, Sky, and Anom, many of their gangster users also sent messages across a free secure messaging app called Wickr. Some of those users worried, might Wickr be next on the list for infiltration?

They never got to find out. Rather than deal with a problematic user base, Wickr decided to close down the free version of its app. In June 2022, an NBC News investigation found Wickr had been cited in more than seventy court cases in which defendants allegedly used the app to trade images of child sexual abuse. On the last day of the year, Wickr then stopped accepting new users and shuttered completely on December 31, 2023.

Child sexual abuse material is the context of the current debate around access to encrypted content. Apple planned, and eventually shelved, a feature that would automatically scan photos stored on users' iPhones that were uploaded to iCloud for child abuse images. Apple scrapped the idea after admitting it saw no way to roll it out without compromising users' security in general. Erik Neuenschwander, Apple's director of user privacy and child safety, said in a memo shared with *Wired* that the scanning would "inject the potential for a slippery slope of unintended consequences. Scanning for one type of content, for instance, opens the door for bulk

surveillance and could create a desire to search other encrypted messaging systems across content types."

Lawmakers in Europe, meanwhile, have pushed for legislation that would mandate monitoring of encrypted messages for that same type of abuse. Before Apple performed a U-turn, privacy activists and cybersecurity researchers repeatedly warned that this sort of scanning could expand to other use cases.

Almost predictably, a Europol official said in a closed-door meeting in July 2022 that "all data is useful and should be passed on to law enforcement," according to minutes of the meeting obtained by the media outlet Balkan Insight. The official added, "There are other crime areas that would benefit from detection and suggested that these could be included." Those comments, when looked at through the lens of the Anom, Encrochat, and Sky operations, show the extraordinary lengths law enforcement is willing to go to circumvent encryption, and how those powers can expand. A superweapon used against child abuse or drug trafficking today could easily be tomorrow's tool for much lesser crimes or stifling protests.

Riana Pfefferkorn, a research scholar at the Stanford Internet Observatory, asked whether secretly running a phone company might be a redline, in a similar way to the debate over facial recognition. As in, is this a technique that society agrees is totally off-limits, or one that can be used with the right guardrails in place? Regardless of the answer to that question, it is a debate that needs to happen in public, Pfefferkorn argued.

"That discussion, I think, needs to happen out in the open, and that means we need to have a full accounting of exactly what it was the FBI did in this situation," she said.

More than anything, Anom pierced the veil of what organized crime looks like today. Anom and the parallel investigations into Encrochat and Sky showed how organized criminals are infinitely resourceful, able to adapt to any obstacle in their way; inseparable from the global system of trade, with tentacles throughout the world's logistics systems; and imbued with an overwhelming power to corrupt officials in positions of power to their own ends.

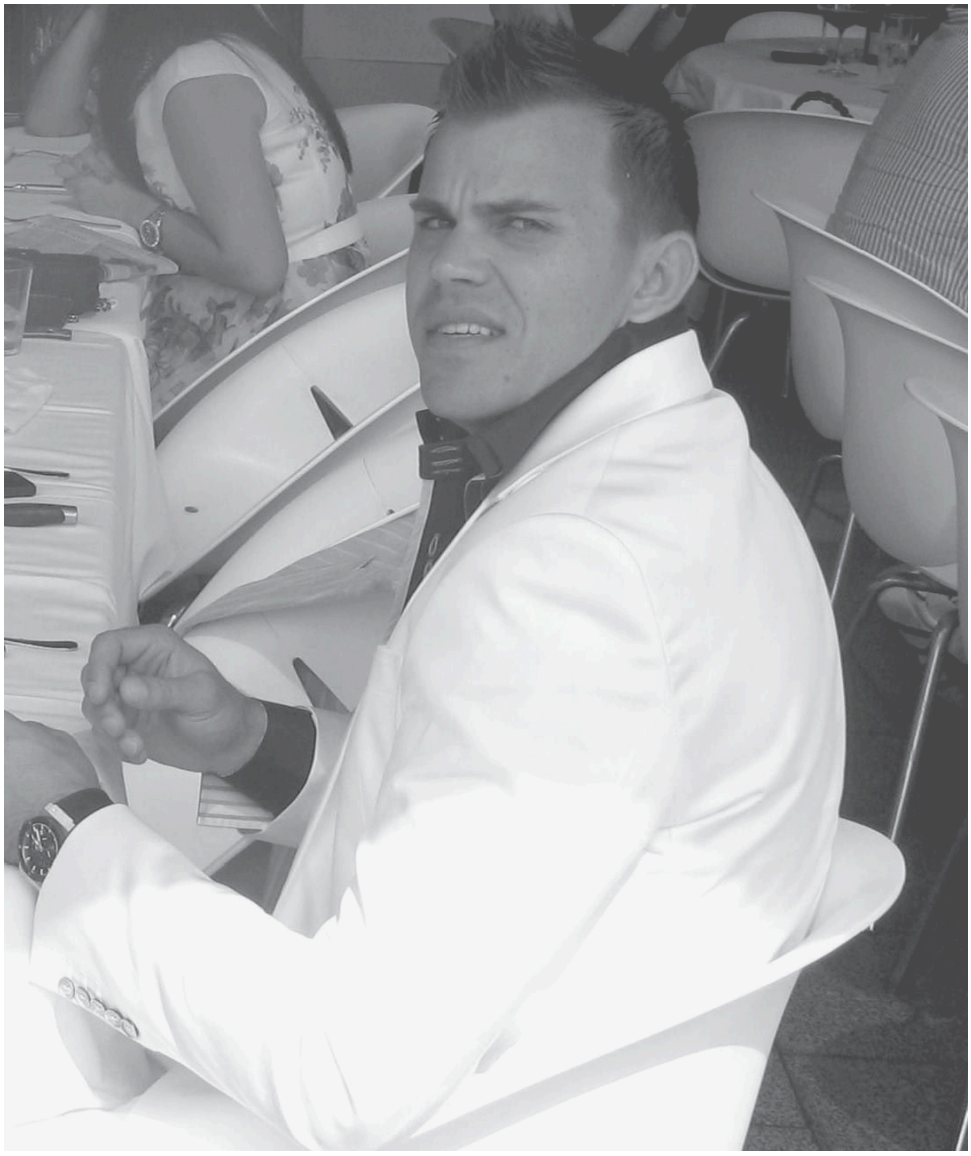
The scale of crime surprised the very law enforcement officials tasked with combating it, causing them in some cases to completely reassess how colossal an issue it really was.

The seizure and arrest numbers from the encrypted phone takedowns are staggering. The Anom, Encrochat, and Sky operations did all stop massive drug shipments and prevented people being killed. That is unambiguous impact. But even Anom, the biggest law enforcement sting in history, did not, and cannot, make a macro level dent in the drug trade. The result, ultimately, was little more than a rounding error on the master spreadsheet behind the global narcotics trade.

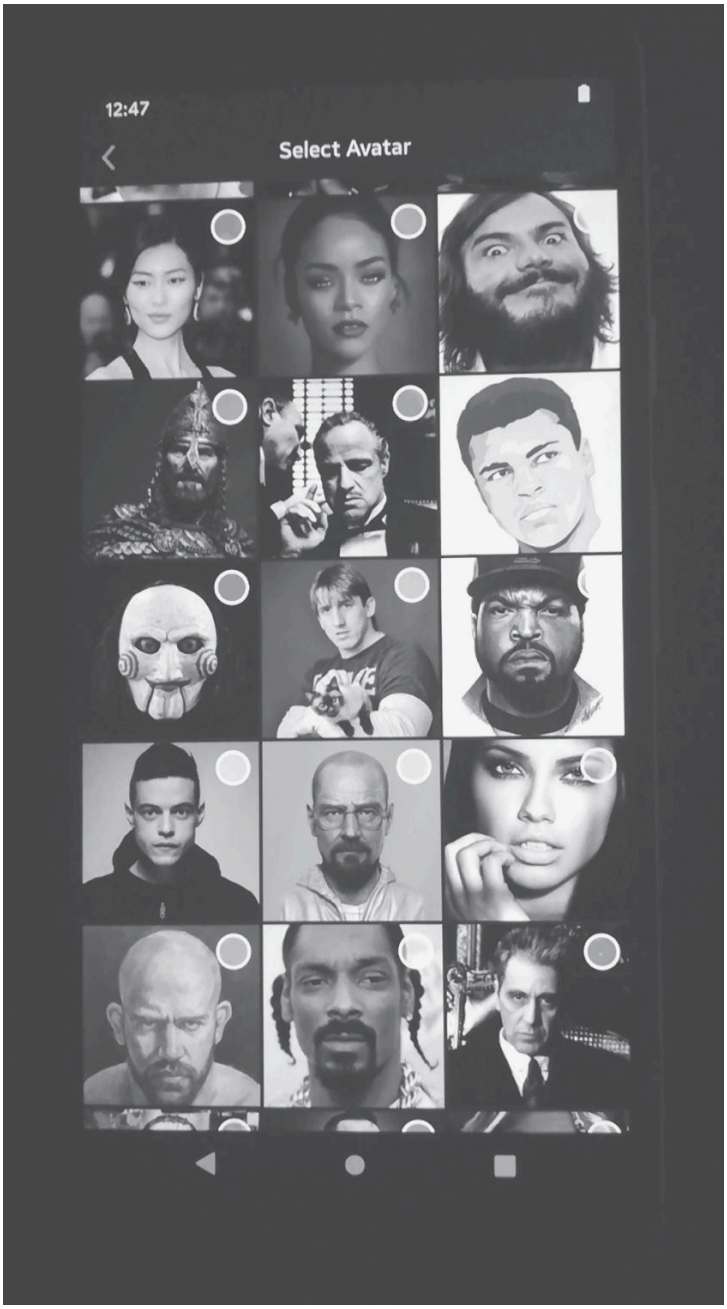
That obviously doesn't mean law enforcement should stop investigating these criminals. But if even such an ambitious operation can't lead to a tangible shift, what possibly can?

One thing is certain. The FBI or its partners will do something like this again.

Toward the end of the conference, Muse said, "There's more work to be done. There's more that we can learn from this. And I hope that we'll figure out whatever the next evolution of Operation Trojan Shield is, and I'm excited for whatever comes next."



Owen Hanson.
Courtesy of the author.



Some of the profile pictures available to Anom users.
Courtesy of the author.

Microsoft stands next to an Anom sign in Turkey.
The Swedish Police Authority.

Body cam footage of Swedish authorities raiding Microsoft's amphetamine lab. *Courtesy of the author.*

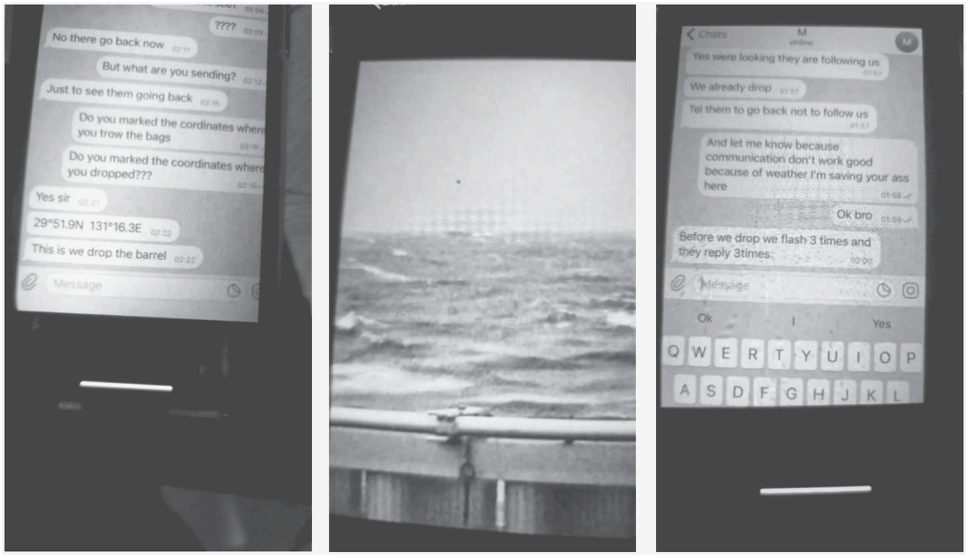
1,595 kilograms of cocaine that were concealed within hollowed-out pineapples. Anom messages led to the seizure.
US Department of Justice.

A block of amphetamine embossed with the word TJACK at Microsoft's request.
The Swedish Police Authority.

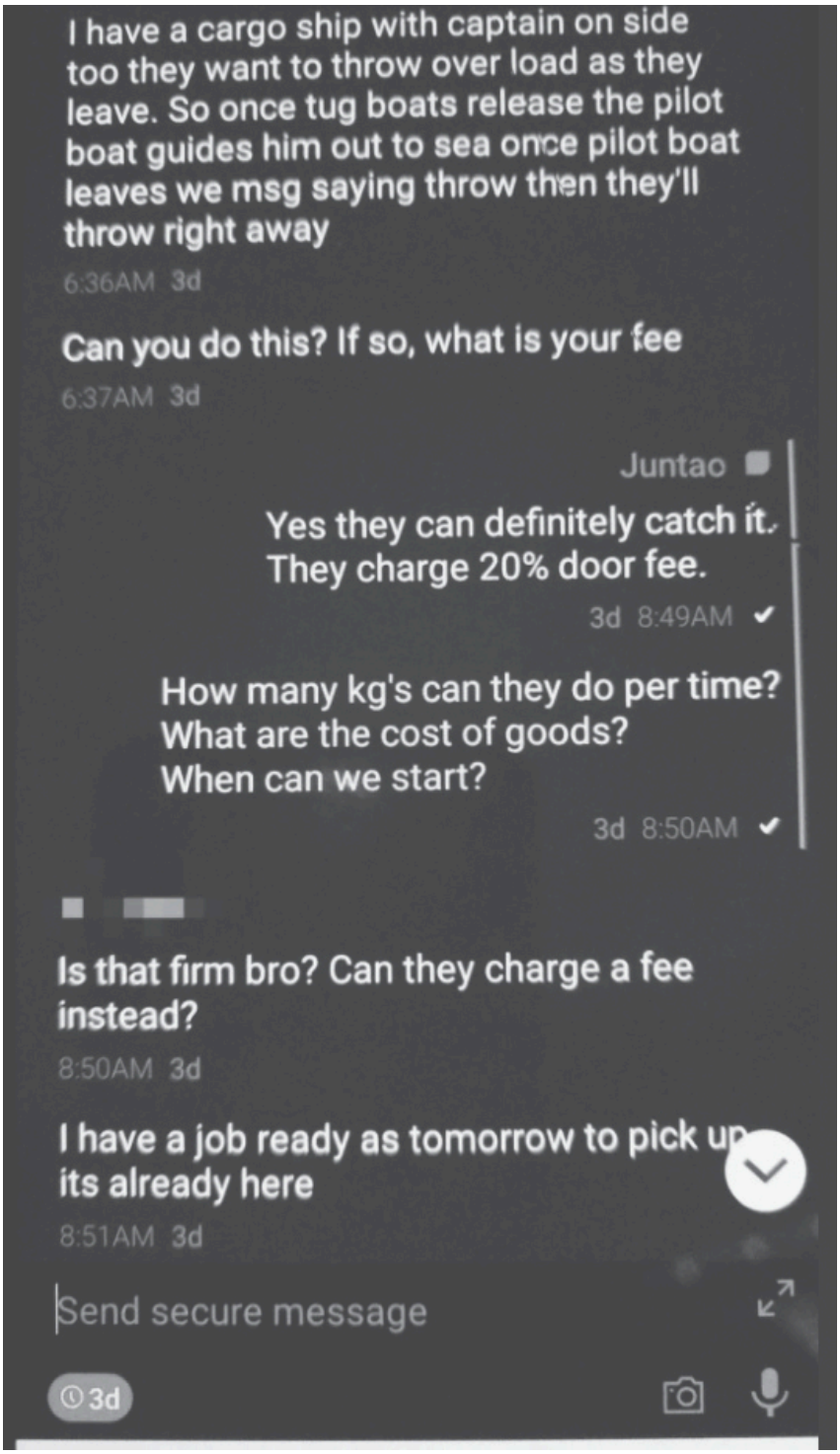
A photo sent across Anom of cash proceeds of illegal transactions.
US Department of Justice.

One of Microsoft's accomplices photographs cocaine smuggled into Sweden via speedboat.
The Swedish Police Authority.

A massive shipment of cocaine hidden inside tuna cans from Ecuador. Anom messages led to the seizure.
US Department of Justice.


????
No there go back now
But what are you sending?
Just to see them going back
Do you marked the cordinates where you trow the bags
Do you marked the coordinates where you dropped???
Yes sir
29°51.9N 131°16.3E
This is we drop the barrel
Message
Chats
Yes were looking they are following us
We already drop
Tel them to go back not to follow us
And let me know because communication don't work good because of weather I'm saving your ass here
Ok bro
Before we drop we flash 3 times and they reply 3times.
Message
Ok
I
Yes
Q W E R T Y U I O P
A S D F G H J K L

WhatsApp messages related to a Microsoft-linked drug job.
The Swedish Police Authority.


I have a cargo ship with captain on side too they want to throw over load as they leave. So once tug boats release the pilot boat guides him out to sea once pilot boat leaves we msg saying throw then they'll throw right away
6:36AM 3d
Can you do this? If so, what is your fee
6:37AM 3d
Juntao
Yes they can definitely catch it. They charge 20% door fee.
3d 8:49AM
How many kg's can they do per time? What are the cost of goods? When can we start?
3d 8:50AM
Is that firm bro? Can they charge a fee instead?
8:50AM 3d
I have a job ready as tomorrow to pick up its already here
8:51AM 3d
Send secure message
3d

Messages captured by Anom.
US Department of Justice.

REWARD

OF UP TO

$5,000,000

FOR INFORMATION LEADING TO THE ARREST AND/OR CONVICTION OF

Maximilian Rivkin

WANTED IN U.S. FOR RACKETEERING CONSPIRACY TO CONDUCT ENTERPRISE AFFAIRS
WANTED IN SWEDEN FOR AGGRAVATED NARCOTICS TRAFFICKING

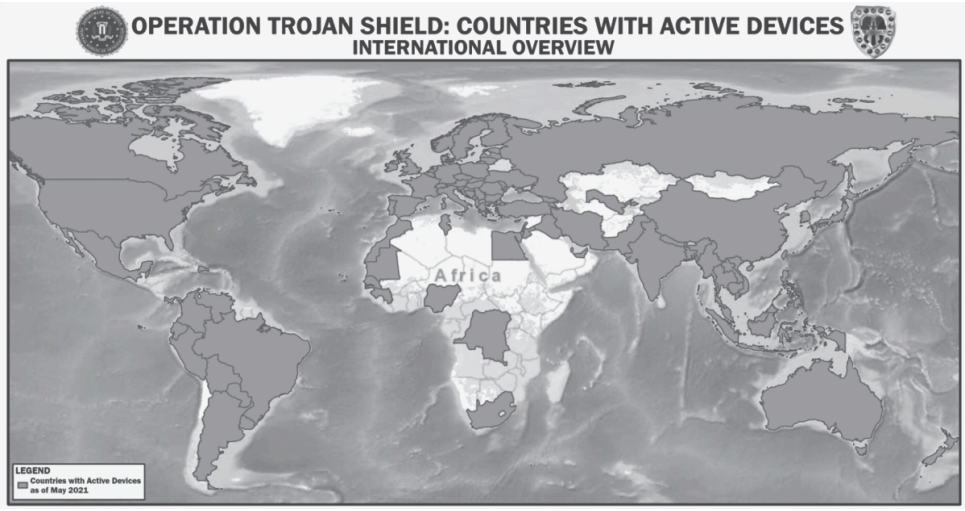
SEND TIPS VIA EMAIL:

SD_Rivkin_Reward@FBI.GOV (FBI)

efterlyst@polisen.se (Swedish Police)

QR Code Link: https://www.state.gov/maximilian-rivkin

A poster offering a $5 million reward for information leading to the arrest and/or conviction of Microsoft.
US State Department.



A map showing countries where Anom devices were active.
US Department of Justice.

Motorbikes seized by Australian authorities during the Joint Action Day.
Australian Federal Police.

An armed officer stands as Australian authorities conduct raids.
Australian Federal Police.

A Note on Sourcing

I first started reporting on the encrypted phone industry in 2016. While much of the privacy, security, and encryption debate at that time was focused on the big tech companies like Apple, I came across something that nobody else seemed to be paying much attention to. On an obscure Dutch crime blog, I read about a company that was taking ordinary BlackBerry phones and installing encrypted email software onto them. As I dug deeper, what I found was an entire ecosystem of phone companies that promised to keep the cops out of their clients' messages, and that in some cases advertised specifically to organized crime. I was blown away. This was where the top criminals must be hiding, I thought. And it was surely where law enforcement would look next, I told anyone who would listen. I kept digging, made the encrypted phone industry one of my focuses, and developed sources among the people who made the phones and the criminals who used them.

It didn't take long for the cops to target that wider industry. The FBI shut down Phantom Secure in 2018, and I published an in-depth investigation about that firm. Then I was the first journalist to reveal the scale of the authorities' hack against Encrochat, another encrypted phone provider, in 2020. And I was the journalist who told the owner of Sky that the Department of Justice had just indicted him in 2021.

In a way, this book is the culmination of that nearly ten years of beat reporting. I've sat in darkened hotel lobbies as encrypted phone sellers handed me USB sticks loaded with information about a competitor. I've walked through city parks in the pitch black to have hushed conversations with people who sell encryption-circumventing tools to governments. I've received threats of physical violence after I published the names of people involved in the phone industry. "Do you realize who you're fucking with?" one read.

But more specifically, I started to work on this book essentially the moment that the US Attorney's Office for the Southern District of California and the San Diego FBI announced it had been secretly running its own encrypted phone company called Anom in June 2021. I was taken aback at how brazen and audacious the FBI's operation was. But at the same time, it was obvious that Anom was the natural next step after shutting down and hacking these companies. Immediately I saw the conclusion of a story I had been obsessed with for years, and the perfect arc for a book: the growth of a shadowy industry into a backbone of organized crime, before law enforcement caught wise and undermined trust in it entirely, with all of the legitimate questions around privacy and surveillance that came with that.

This is to say that although I do not appear as a character in the book, it is based on my countless conversations with people inside this world. I did not want to distract readers by inserting myself into the narrative where it was not necessary. This book is already about the largest sting operation in history—I would much prefer to tell it through the eyes of the people who were there, inside Anom. The references section includes many articles from other journalists that were invaluable for confirming specific details. But the vast, vast majority of the material in this book is based on my own investigative reporting and has not been published before.

That includes extensive interviews with people from every aspect of the story of Anom: fugitives wanted by the FBI; members of organized criminal groups; convicted drug traffickers; current and former law enforcement officials in the United States, the Netherlands, Sweden, Australia, and other countries; as well as coders, developers, and sellers for Anom and other encrypted phone companies.

Most people mentioned in this book have had a chance to comment. But just because I quote or describe a specific person, a reader should not assume they were a source of mine, either in general or for that particular scene. When reporting on organized crime and government surveillance operations, I have to be extremely careful that my sources' identities remain a secret. The majority of these sources took great professional or personal risks by speaking to me. Some had signed NDAs that barred them from communicating with the press. Others would likely be killed or seriously harmed if it became known they were a source of mine. And some of my

sources are still being hunted by the authorities, meaning they put their freedom on the line by telling me their story.

I have changed the names of some subjects, usually to protect them from retaliation from violent organized criminals or law enforcement. The changed names are clearly labeled by footnotes in the text.

Unless specified, at the time of writing, criminal cases against many subjects in this book are ongoing, and, in the eyes of the courts, the described activity is alleged.

All scenes in this book are based on interviews with people who have direct knowledge of those events or other supporting material. That material includes tens of thousands of pages of Anom messages I obtained and read over the course of months; photos and videos; court records; police surveillance reports; and leaked text message and email conversations from inside Anom. For the material from within Anom, I have verified these documents by showing them to other independent Anom-related sources, who confirmed their authenticity. I have also performed forensic analysis to corroborate certain technical details, including reverse-engineering the Anom app itself to find clues on how it was made.

Thankfully, this book also gave me opportunities to leave my desk and computer. I managed to get into a law enforcement and industry-only conference in Vancouver where two of the FBI agents involved gave a candid presentation about the Anom operation, and parts of the quoted material come from that event. Later I stood inside some of the very rooms in the San Diego FBI's field office where agents read the millions of messages harvested by Anom. I walked the halls of the US Attorney's Office in downtown San Diego. I met people face-to-face in multiple countries who sold Anom phones to organized criminals.

All sources have motivations for speaking to journalists. In the case of this book, some of the people felt like used pawns in a much larger game and didn't want their voice to be stamped out. Others were the chess players and were proud of what they achieved. Some found catharsis in telling someone their side of the story when they hadn't yet had an opportunity to do so. Beyond the people quoted in the book either under their name or a pseudonym, I spoke to many more off the record, simply for my own understanding of the story.

There is very little investigative journalism without sources. And there is no narrative journalism without sources who painstakingly explain their story again and again, even when a journalist calls to ask the most trivial or pedantic question. I am forever grateful to everyone who spoke to me for this book, and who trusted me to tell what I think is the most significant true crime story of the twenty-first century so far.

Acknowledgments

I will always be thankful to my sources first and foremost. But this book would not exist if not for a number of other people as well.

Bradley Hope, coauthor of *Billion Dollar Whale* and *Blood and Oil* and author of *The Rebel and the Kingdom*, was the first person who told me I should turn my reporting on the encrypted phone industry into a book. Without his encouragement I don't know if I would have taken the plunge.

At the time of writing the book, I was a senior staff writer at *Motherboard*, the technology section of Vice Media. My editors there, Jason Koebler and Emanuel Maiberg, pushed internally for me to receive book leave. I don't want to imagine what the writing process would have been like without that time to focus on the book, and I'm grateful that they ensured I got it.

My fact-checker Matthew Giles was a godsend. He caught details that I had not thought of and tidied my phrasing to make it as accurate as possible. The book is undoubtedly sharper and richer because of his work.

Max Karlsson was my Swedish translator. His work was crucial for making sure that dialogue in many scenes was accurate, especially those involving Microsoft and his associates.

Anom was a global operation, so it is impossible for one person to cover every single aspect. With that in mind, the journalist Mitch Mott patiently helped me better understand the fallout from the Anom operation in Australia specifically. Chris Bing from Reuters gave me the initial tip that the FBI was speaking about its operation at a law-enforcement- and industry-only conference in Vancouver. Tom Kington and Antonio Nicaso pointed me to certain details about the arrest of Morabito that I then managed to expand upon.

Thank you to my agent Eric Lupfer, who immediately saw how crazy this story really was and put his full might behind finding a home for it.

And the same goes for Tara Timinsky, an incredible agent who was instrumental in having Netflix acquire the rights to the book.

A huge thanks to everyone at my publisher, PublicAffairs. They include my editor Benjamin Adams, who understood what the Anom story showed about the globalized nature of organized crime, and who kept me on track to communicate the massive stakes of this operation; and Kelly Lenkevich for shepherding me through the production process. Thanks also to Jennifer Top, who beautifully copyedited the book.

Several friends kindly read early sections of the book and provided feedback. Those include Lorenzo Franceschi-Bicchierai, who helped with my original book pitch, even printing it out on paper and scribbling notes in the margin. He also assisted with Spanish and Italian translations. Andy Greenberg, author of *Tracers in the Dark* and *Sandworm*, read certain scenes and provided invaluable feedback on making complex topics come to life. Other friends gave help and pointers along the way. They include Mike Isaac, author of *Super Pumped*, and Samantha Cole, author of *How Sex Changed the Internet*.

Finally, thank you to my family and to M for listening to me speak about this project for years and years, both when I was stressed to my wits' end or excited beyond belief. I could not have written this without your undying support.

Discover Your Next Great Read

Get sneak peeks, book recommendations, and news about your favorite authors.

Tap here to learn more.

PUBLICAFFAIRS

Photo courtesy of the author

Joseph Cox is an award-winning investigative journalist who has made a career uncovering how organized crime really works and exposing government surveillance programs. He has been the world's leading reporter on the Anom story, publishing a series of exclusive stories about it for Vice Media's *Motherboard*. He appears with frequency on NPR, NBC, and the BBC, and has done extensive speaking at dozens of conferences related to the tech, security, business, and communications subjects intersecting with the book. He is also a cofounder of 404 Media.

Praise for

DARK WIRE

"Joseph Cox has written an instant true-crime classic, the inside—very inside, it turns out—story of the largest global crime sting in history, a fascinating portrait not just of the frontiers of technology, but also how organized crime operates in the twenty-first century. Filled with stranger-than-fiction gangsters and smugglers, this book is part *Miami Vice*, part *Sneakers*, and part *Ocean's Eleven*. Your eyebrows will be raised in amazement page after page."

—Garrett Graff, director, Cybersecurity Program, Aspen Institute, and bestselling author of *Watergate*

"A jaw-dropping page-turner that truly terrified me. The story of how the FBI subverted an encrypted messaging program should send chills down the spine of anyone who cares about privacy and a free society."

—Julia Angwin, contributing writer, *New York Times*, and bestselling author of *Dragnet Nation*

"A tense, deep, beautifully told tale that could be a top-notch technothriller.… Except it's all true."

—Cory Doctorow, author of *The Bezzle* and *The Internet Con*

"Cox has pulled off a breathtaking feat of reporting. He brings readers into the very rooms where the criminal underworld's most audacious conspiracies are planned and executed—and into the rooms where the cops are watching it all. His book is true to its namesake, *The Wire*, but more real, more raw, and played out at a staggeringly global scale."

—Andy Greenberg, senior writer, *Wired*, and author of *Tracers in the Dark* and *Sandworm*

"One of the best true-crime thrillers I've read in years. With its tremendously flawed and persistent characters and crazy plot, it felt instantly like a television show while also illuminating the way the shadowy underworld uses encrypted and special phones."

—Bradley Hope, coauthor of *Billion Dollar Whale* and *Blood and Oil*

Notes

Chapter 1: ODOG

Nusbaum, Eric. “Unusual Suspect: The Rise and Fall of Owen Hanson, Former USC Athlete and Alleged Drug Kingpin.” *Vice*, December 1, 2016.

Chapter 3: Boxes of Phantoms

Berger, Meyer. “Tapping the Wires.” *New Yorker*, June 11, 1938.

Canwest News Service. “Criminals Pick BlackBerries to Thwart Eavesdropping Police.” Canada.com, October 8, 2007.

Ling, Justin, and Jordan Pearson. “Exclusive: Canadian Police Obtained BlackBerry’s Global Decryption Key.” *Vice News*, April 14, 2016.

Statista. “Number of Blackberry Smartphone Users in the United States from 2010 to 2021.” March 2019.

Stewart, Sinclair. “RBC’s BlackBerry-Addicted Feel Withdrawal Pangs.” *Globe and Mail*, March 11, 2005.

Chapter 4: The Facebook Gangster

ABC News. “Six Charged After Drug Bust Which Seized 2.8 Tonnes of MDMA and Methamphetamine Worth $1.5 Billion.” November 28, 2014.

ABC News. “Sydney Shooting Victims Targeted in Deliberate Hit.” August 30, 2012.

Australian Criminal Intelligence Commission. “ACIC 2017–18 Annual Report.” October 11, 2018.

Australian Criminal Intelligence Commission. “Organised Crime in Australia 2017.” 2017.

Baker, Richard, and Nick McKenzie. “Fugitive Bikie Suspected of Setting Up Industrial-Scale Meth Lab in India.” *Sydney Morning Herald*, March

25, 2012.
Bashan, Yoni. “Spanish Bungle Arrest of NSW Drug Lord Hakan Ayik.” *Perth Now*, October 27, 2012.
Benny-Morrison, Ava. “Drug Lord Joseph Hakan Ayik’s $4m Property Empire to Be Seized.” *Daily Telegraph*, April 20, 2020.
Charalambous, Charlie. “Cyprus North-South Crossings Reopen as Covid Curbs Eased.” AFP News, June 4, 2021.
Crawford, Barclay. “Aussie ‘Drug Baron’ Hakan Ayik Arrested.” *The Advertiser*, December 26, 2010.
Cyprus Mail. “Escape Route Blocked for Alleged Drug Lord.” November 16, 2010.
Daily Sabah. “Drug Suspect Wanted in Australia Bailed in N. Cyprus.” December 31, 2010.
Macey, Richard, and David Monaghan. “From the Archives, 1984: The Milperra Bikie Massacre.” *Sydney Morning Herald*, September 3, 1984.
McKenzie, Nick, Joel Tozer, and Sumeyya Ilanbey. “How We Tracked Down Australia’s Most Wanted Man to His Glamorous New Life.” *Sydney Morning Herald*, June 5, 2021.
McKenzie, Nick, and Dylan Welch. “On the Run and on Facebook: Wanted Man Flees Cyprus.” *Sydney Morning Herald*, November 16, 2010.
Miranda, Charles. “Facebook Gangster Hakan Ayik Emerges as Allegedly Australia’s Biggest Drugs Trafficker.” News Corp Australia Network, February 11, 2018.
Morri, Mark. “Passion for Power yet Destined to Die: The Life and Times of Mick Hawi.” *Daily Telegraph*, September 12, 2020.
New South Wales Crime Commission. “Annual Report 2014–2015.” October 26, 2015.
Rose, Anton. “How ‘Most Wanted Man’ Hakan Ayik Got Away from Police in 2010.” *Daily Telegraph*, January 8, 2023.
Tullis, Ashleigh. “Jiun Loong Chai Sentenced over ANOM Drug Sting, Links to Hakan Ayik.” *Daily Telegraph*, November 7, 2022.
Welch, Dylan. “Uncrackable Phones Provided by Phantom Secure Linked to Murder of Hells Angels Bikies.” ABC News, March 5, 2014.
Wells, Jamelle. “Bikie Boss Guilty of Murder over Airport Brawl.” ABC News, November 1, 2011.

Whinnett, Ellen. “Police Believe Ayik Signed Off on Assassinating Comanchero Bikie Buddy Buddle.” *The Australian*, January 15, 2023.

Chapter 7: Face-to-Face

Mitchell, Peter. “Aust, NZ Secrets May Have Been Leaked.” *Canberra Times,* September 16, 2019.

Tunney, Catharine. “Lawyer for RCMP Official Accused of Leaking Secrets Seeks a Stay of Proceedings.” *CBC,* March 3, 2022.

Chapter 8: The Capturing of Vincent Ramos

Mitchell, Peter. “Canadian Who Sold Uncrackable Phones to Australian Gangs Jailed.” *Sydney Morning Herald,* May 29, 2019.

Chapter 9: Vacuum

Cox, Joseph. “‘We Have to Run a Good Company’: How the FBI Sold Its Encryption Honeypot.” *Motherboard*, June 9, 2021.

Chapter 10: Anom

News.com.au. “The Moment AFP Tech Genius Blew Up the Underworld in His Bare Feet.” *NewsDNA*, June 8, 2021.

Chapter 11: Roll Out

9 News. “‘Respectful’ Man Avoids Jail over Drug Lab.” November 28, 2016.

De Nadai, Natalie. “Olive Producer Domenic Catanzariti Shares the Secrets to a Top Olive.” *The Advertiser*, July 17, 2014.

Mott, Mitch. “Alleged Comanchero Member Refused Bail Despite Claiming He Lost 31kg Behind Bars Because of Sleep Apnoea.” *The Advertiser*, May 26, 2022.

Opie, Rebecca. “Man Avoids Jail over $10-Million Drug Bust Due to ‘Lack of Criminal History.’” ABC News, November 28, 2016.

Tan, Qiuyi. “Entertainer Who Took $416k Worth of Gold Bars to Turkey Keeps Identity Secret Until Trial.” *New Zealand Herald*, June 3, 2022.

Whinnett, Ellen. “Part 3: Criminal ‘Influencers’ Who Took the AFP and FBI Bait by Using the AN0M App.” News Corp Australia Network, June 8, 2021.

Chapter 12: Hoops

Cox, Joseph. “Revealed: The Country That Secretly Wiretapped the World for the FBI.” 404 Media, September 11, 2023.

Chapter 13: Batman

Calvey, Mark. “Pulse Tragedy, Hurricane Top of Mind at LGBT Nonprofit’s Summit in Orlando.” *Orlando Business Journal*, October 6, 2016.

Chapter 14: Kings Cross

Cox, Joseph. “Inside the Phone Company Secretly Run by Drug Traffickers.” *Motherboard*, October 22, 2019.

Fife-Yeomans, Janet, and Mark Morri. “Comanchero Ex-Pat Marco Coffen Bags Ciphr Encryption Rights for Oz.” *Daily Telegraph*, November 16, 2020.

McKenzie, Nick, Joel Tozer, and Fergus Hunter. “The Cartel of Australian Mr Bigs Responsible for $1.5b Drug Imports.” *Sydney Morning Herald*, June 6, 2021.

Miranda, Charles. “Facebook Gangster Hakan Ayik Emerges as Allegedly Australia’s Biggest Drugs Trafficker.” News Corp Australia Network, February 11, 2018.

Mott, Mitch. “AFP Documents Reveal the ‘Astronomical Wealth’ of Facebook Gangster and AN0M Distributor Hakan Ayik.” *The Advertiser*, June 29, 2023.

Chapter 15: Microsoft

Dagens Nyheter. “FBI: Svensk 37-åring centralfigur i Anom-nätverket.” June 9, 2021.

El Periódico. “Expulsan de Colombia a sueco que protagonizó escándalo en hotel de Cartagena.” May 22, 2019.

The Europol Podcast. “Operation Greenlight Part 2: Action Day.” Europol, August 22, 2022.
Porras, Yessica Rivera. “‘A los extranjeros les exigimos respeto por nuestras normas’: Pedrito Pereira.” *El Universal*, June 29, 2019.
Ramirez, Maria Fernanda. “Liquid Cocaine—a Rising Trend Among Colombia’s Traffickers.” InSight Crime, February 9, 2022.
Reyntjens, Sam. “Colombia uitgezet, gewapend betrapt in Brasschaat en gezocht door de FBI, Zweedse gangster riskeert vier jaar cel in Antwerpen.” *Het Nieuwsblad*, March 9, 2023.

Chapter 16: Encrochat

Cox, Joseph. “Encrypted Phone Network Says It’s Shutting Down After Police Hack.” *Motherboard*, June 22, 2020.
CrimeSite. “Pgp-chatservice Encrochat gehackt door een overheidsdienst.” June 13, 2020.
Duffy, Tom, and Leigh Mcmanus. “Gang Brothers and ‘England Footballer Lookalike’ Among Brit Dealers Busted by Encro Hack.” *Daily Star*, December 29, 2022.
Everett, Adam. “Cocaine Deal Broker and Debt Collector Splashed Out on Rolex for His Birthday.” *Liverpool Echo*, November 14, 2022.
Everett, Adam. “Criminals Who Felt the Wrath of Their Rivals Were Stabbed and Tortured.” *Liverpool Echo*, December 25, 2022.
Everett, Adam. “Secret Drug Plots of ‘Big Dunc,’ ‘Musical Salmon,’ ‘Educated Goose’ and ‘Heroic Fox.’” *Liverpool Echo*, December 25, 2022.
Fetherstonhaugh, Neil. “‘Glamorous’ UK Police Officer Claimed She Didn’t Know Her Husband Was Drug Lord.” *Sunday World*, December 13, 2022.
Humphries, Jonathan, and Sarah Vesty. “Royal Marine Drug Dealers Snared After Thousands of EncroChat Messages Uncovered.” *Liverpool Echo*, December 5, 2022.
Mare, Tess de la. “Trio Jailed over £3m Cocaine-Running Plot.” BBC News, November 1, 2022.
McNeill, Heather. “Perth Criminal Lawyer, WA Bikies Caught Up in AFP and FBI ‘Sting of the Century.’” *WA Today*, June 9, 2021.

Nicholson, Abigail. “Former Liverpool Player Jailed for Part in Encrochat Gang.” *Liverpool Echo*, October 18, 2022.
Seaward, Tom. “Drug Gang Foot Soldier ‘StaySharp’ Handled Cocaine Worth £1m.” *Oxford Mail*, December 13, 2022.
Summers, Chris. “EncroChat Hack by French Was Law Enforcement Equivalent of ‘D-Day Landings,’ UK Tribunal Told.” *Epoch Times*, December 16, 2022.

Chapter 17: “We Move Anom Like We Move Kilos”

Henley, Jon. “Sweden’s Gun Violence Rate Has Soared Due to Gangs, Report Says.” *Guardian*, May 26, 2021.
Orange, Richard. “Bombs and Blood Feuds: The Wave of Explosions Rocking Sweden’s Cities.” *Guardian*, January 25, 2020.
Townsend, Mark. “How the Murder of a Swedish Rapper Shocked a Nation and Put Police on the Back Foot.” *Guardian*, December 4, 2021.

Chapter 18: “Let’s Make Millions”

9News Staff. “Police Find 20kg of Cocaine Hidden in Secret Safe Inside Welding Machines.” 9News, September 9, 2020.
Hunt, Nigel. “How Operation Ironside Thwarted an Alleged Murder Plot Involving a Machine Gun and an Ambush on Norwood Parade.” *Daily Telegraph*, June 8, 2021.
Mott, Mitch. “Tereapii Pokoina Pleads Guilty to $20m Cocaine Haul Intercepted as Part of Operation Ironside.” *The Advertiser*, June 1, 2022.

Chapter 19: Wasta

Agence France-Presse. “Dubai Police Arrest Netherlands’ Most Wanted Man.” *Guardian*, December 16, 2019.
Cavanagh, Niamh. “NO ESCAPE Billy Hood—Inside Dubai Hellhole Jail Holding Brit Footballer Where Inmates Are Tortured and Left to Die from Diseases.” *US Sun*, October 21, 2021.
Dosja, Nga. “‘E pamundur ta hakosh!’/ Eldi Dizdari i kujdesshëm në detaje, pajisi gjithë grupin me ‘BlackBerry’, DY aplika.” Dosja, September 17, 2020.

Eurojust. “Eurojust Annual Report 2020.” 2021.
Lala, Klodiana. “Albanian Crime Story: Hostage to the Cocaine Supply Chain.” *Balkan Insight*, July 1, 2021.
Morri, Mark. “Alleged Drug Kingpins’ Escape from Dubai Jail Foiled by AN0M App.” *Daily Telegraph*, June 9, 2021.
NL Times. “Taghi Part of ‘Super Cartel’ Controlling Third of EU Cocaine Trafficking: Report.” October 18, 2019.
Sherry, Alan. “REVEALED: How Kinahan Ally Raffaele Imperiale Used Encrypted Phones to Move Millions in Cash and Drugs.” *Sunday World*, January 28, 2023.
Siracusa International Institute. “Closing the Implementation Gap.” November 2020.
Turak, Natasha. “UAE Loosens Some VoIP Restrictions as Residents in Lockdown Call for End to WhatsApp and Skype Ban.” CNBC, March 26, 2020.

Chapter 21: A Cottage Industry

EMCDDA. “European Drug Report Trends and Developments 2022.” Publications Office of the European Union, 2022.
Duffin, Perry. “Inside the Firm: How an International Drug Cartel Plotted a ‘Line to Australia.’” *Sydney Morning Herald*, April 16, 2023.
Kruithof, Kristy, Judith Aldridge, David Décary Hétu, Megan Sim, Elma Dujso, and Stijn Hoorens. “Internet-Facilitated Drugs Trade: An Analysis of the Size, Scope and the Role of the Netherlands.” Santa Monica, CA: RAND Corporation, 2016.

Chapter 23: Metallic Maze

AFP. “Belgium Needs More Incinerators to Burn Seized Cocaine.” *Guardian*, November 21, 2022.
Agence France-Presse. “Four Arrested over Alleged Plot to Kidnap Belgian Justice Minister.” *Guardian*, September 25, 2022.
Bertha, Aymon. “Vrej Yezekellian Sentenced, Leaving Kigham Wartanian Waiting for Verdict for Attempting to Import Cocaine.” *Daily Telegraph*, February 24, 2023.

Brussels Times. "'Belgium Has Entered into Narco-Terrorism,' Says Justice Minister." September 28, 2022.
Carter, Dylan. "Over a Quarter of Cocaine Seized in Latin American Ports Destined for Antwerp." *Brussels Times*, October 22, 2022.
EMCDDA. "European Drug Report Trends and Developments 2021." Publications Office of the European Union, 2021.
EMCDDA. "European Drug Report Trends and Developments 2022." Publications Office of the European Union, 2022.
Guarascio, Francesco. "Europe Flooded with Cocaine Despite Coronavirus Trade Disruptions." Reuters, April 30, 2020.
Lyons, Helen. "Belgium Ranks 5th Worldwide on Ports of Entry for Counterfeit Containers." *Brussels Times*, March 5, 2021.
Marson, James. "Inside Europe's Cocaine Gateway: 'A Repeat of Miami in the 1980s.'" *Wall Street Journal*, December 31, 2021.
Marson, James. "Massive Hack Gave Police a Window on Cocaine, Cash and Killers." *Wall Street Journal*, November 23, 2021.
Redacción Digital. "Golpe al narcotráfico: Se detuvo un contenedor con 8.670 latas circulares que contenían droga." TC Television, October 3, 2020.
Reuters staff. "Traffic to Antwerp Port Blocked as Cargo Ship Runs Aground." Reuters, August 14, 2017.
Torfs, Michaël. "Justice Minister: 'We Are in a New Phase, One of Narco-Terrorism.'" *VRT*, September 28, 2022.
UNODC and EUROPOL. "The Illicit Trade of Cocaine from Latin America to Europe—from Oligopolies to Free-for-All?" UNODC, September 2021.
Van den Berghe, Caroline, and Joris Truyts. "3 Nederlanders opgepakt voor ontvoeringspoging tegen minister Van Quickenborne, vierde verdachte nog op de vlucht." *VRT*, September 24, 2022.
Zoutberg, Amée. "Three Explosions in Antwerp May Be Related to Drug Gang Conflict." *Brussels Times*, August 24, 2020.

Chapter 24: Hawala

EUROPOL. "EUROPOL SOCTA 2013. EU Serious and Organised Crime Threat Assessment." European Police Office, 2013.

EUROPOL. “Why Is Cash Still King? A Strategic Report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering.” European Police Office, 2015.
Parkes-Hupton, Heath. “The AFP Turns Its Focus to Crushing the ‘Lifeblood’ of Organised Crime in Australia—Money Laundering.” ABC News, March 16, 2023.
United Nations. “International Narcotics Control Board Report 2021.” UN International Narcotics Control Board, January 2022.

Chapter 25: Black Boxes

Chung, Laura, and Fergus Hunter. “Nephews of Australia’s Most Wanted Man Swept Up in Global App Sting.” *Sydney Morning Herald*, June 10, 2021.
Mazzoni, Alana. “Bikies, Fugitives and Glamorous Girlfriends: Inside the VIP Dinner in Istanbul as Top Comancheros Mingled with an On-the-Run Drug Lord to Celebrate His Wife’s Birthday—as Gang Is Exposed by AN0M Sting.” *Daily Mail*, June 9, 2021.
Pandaram, Jamie. “Former Comanchero Boss Fidel Tukel Talks About Why He Walked Away.” *Saturday Telegraph*, May 28, 2022.
Whinnett, Ellen. “Operation Ironside: Former Bikie Baris Tukel Pictured at Dinner with Fugitive Drug Lord Hakan Ayik.” News Corp Australia Network, June 9, 2021.

Chapter 26: Juggernaut

Cox, Joseph. “Encrypted Phone Firm ‘Sky’: Someone Sold Compromised Versions of Our App.” *Motherboard*, March 9, 2021.
Cox, Joseph. “Indicted CEO of Encrypted Phone Firm ‘Sky’ Says He Will Clear His Name.” *Motherboard*, March 14, 2021.
Debels, Thierry. “Gerecht kraakt ‘onkraakbare’ berichten van SKY ECC van drugsdealers en valt op ruim 200 plaatsen binnen.” *P-magazine: PNWS*, March 9, 2021.
Eeckhaut, Mark. “Zware klap voor georganiseerde misdaad: gerecht hackt ‘onkraakbare’ misdaadtelefoons.” *Der Standaard*, March 9, 2021.
Marson, James. “Massive Hack Gave Police a Window on Cocaine, Cash and Killers.” *Wall Street Journal*, November 23, 2021.

Murray, David. “Organised Crime Hangs Up on Ciphr.” *The Australian*, March 16, 2021.
Roudik, Peter. “Russia: Import of Blackberry Phones Permitted.” *Newsline*, February 26, 2008.

Chapter 28: Green Light

BBC. “Rocco Morabito: Italian Fugitive Arrested in Brazil.” May 25, 2021.
Elliott, Lucinda, and Tom Kington. “King of Cocaine Rocco Morabito Caught Basking in the Sun After 30 Years on Run.” *Times*, May 29, 2021.
EUROPOL. “Complexities and Conveniences in the International Drug Trade: The Involvement of Mexican Criminal Actors in the EU Drug Market.” EUROPOL and the DEA, December 5, 2022.
Miller, Greg. “‘The Intelligence Coup of the Century.’” *Washington Post*, February 11, 2020.

Chapter 29: Hydra

Hunt, Nigel. “How Operation Ironside Thwarted an Alleged Murder Plot Involving a Machine Gun and an Ambush on Norwood Parade.” *Daily Telegraph*, June 8, 2021.
Mott, Mitch. “Accused Drug Trafficker George Katsambas Told Co-accused AN0M App Was ‘Bad.’” *The Advertiser*, July 16, 2021.
Tshikalange, Shonisani. “R400m Cocaine-in-a-Boat Accused Linked by ‘Encrypted App’ Anom.” *Sowetan Live*, August 24, 2021.

Chapter 30: Mancuso Luck

Perpitch, Nicolas. “Three Luxury Cars, $1 Million Seized in WA Organised Crime Probe as Trio Faces Court.” ABC News, November 20, 2020.
Ryan, Hannah. “16-Year-Old Among 10 People Charged over Alleged Violent Home Invasion and Kidnapping in Western Sydney.” 7News, June 1, 2021.
Steger, Sarah. “Ex-Lone Wolf Bikie Dillan Mancuso’s Bail Revoked at His Request.” *West Australian*, December 7, 2021.

Epilogue

Australian Associated Press. “Comanchero Bikie Boss Mark Buddle Arrested in Darwin After Being Deported from Turkey.” *Guardian*, August 2, 2022.

Bayer, Kurt. “Comancheros Member Shane Ngakuru, Identified in FBI Fake Apps Sting, Arrested in Thailand.” *New Zealand Herald*, October 18, 2022.

Cormack, Lucy, and Nick McKenzie. “Turkish Police Arrest Hakan Ayik, Others in International Organised Crime Operation.” *Sydney Morning Herald*, November 2, 2023.

Cox, Joseph. “Apple Delays Release of Child Abuse Scanning Tech After Backlash.” *Motherboard*, September 3, 2021.

Cox, Joseph. “Crime Boss or Tech CEO? An Encrypted Phone Company Sues the Government to Save Itself.” *Motherboard*, November 18, 2021.

Cox, Joseph. “Encrochat Lawyers Say Clients Haven’t Had Fair Trials.” *Motherboard*, February 18, 2022.

Cox, Joseph. “Encrypted Phone Firm Ciphr Plans to Shut Down.” *Motherboard*, August 26, 2022.

Cox, Joseph. “Encrypted Phone Firm Ciphr, Used by Criminals, Moves to Cut Off Australia.” *Motherboard*, September 13, 2021.

Cox, Joseph. “‘Untouchable’: Associates React to Arrest of Drug Trafficker Turned ‘Encryption King.’” 404 Media, November 6, 2023.

Cox, Joseph, and Max Daly. “Cops Investigating ‘WhatsApp for Gangsters’ Arrest Key Suspect in Caribbean.” *Vice News*, June 29, 2022.

Daly, Max. “The EncroChat Hack Was Hailed as a Major Coup Against Gangsters. But Europe Is Still Awash with Drugs.” *Vice News*, June 23, 2022.

Driessen, Camil, and Jan Meeus. “Vertrouwelijke berichten advocaten en hun cliënten tegen wet in toch bewaard.” NRC, April 4, 2022.

Fair Trials. “EncroChat Hack: Fair Trials Denounces Decision of French Court.” April 8, 2022.

Fair Trials. “German Courts Refer the Legality of EncroChat Evidence to the CJEU.” November 8, 2022.

Fotiadis, Apostolis, Luděk Stavinoha, and Giacomo Zandonini. “Europol Sought Unlimited Data Access in Online Child Sexual Abuse Regulation.” Balkan Insight, September 29, 2023.

Goggin, Ben. “Wickr, Amazon’s Encrypted Chat App, Has a Child Sex Abuse Problem—and Little Is Being Done to Stop It.” NBC News, June 10, 2022.

Goggin, Ben. “Wickr Me, Amazon’s Encrypted Chat App, Stops Accepting New Users.” NBC News, January 1, 2023.

Goodwin, Bill. “Chat Control: EU Lawyers Warn Plans to Scan Encrypted Messages for Child Abuse May Be Unlawful.” *Computer Weekly*, May 8, 2023.

Goodwin, Bill. “Italian Supreme Court Calls for Prosecutors to Disclose Information on Sky ECC Hacking Operation.” *Computer Weekly*, October 5, 2022.

Hamadé, Kassem. “Jakten på Said Sadat—så hittades 24-åringen.” *Expressen*, July 5, 2022.

Juanola, Marta Pascual, and Erin Pearson. “Security Concerns to Delay Return of Fugitive Bikie Boss Mark Buddle.” *Sydney Morning Herald*, August 3, 2022.

Morri, Mark. “Duax Ngakuru Takes International Reins of Comanchero Bikies, Living in Turkey.” *Daily Telegraph*, January 1, 2023.

Morri, Mark. “Exiled Sydney Bikie Boss Mark Buddle Flees Dubai for Iraq.” *Daily Telegraph*, June 9, 2021.

Morri, Mark. “New Comanchero Supreme Commander Arrested in Turkey.” *Daily Telegraph*, January 15, 2023.

Mott, Mitch. “Justice Adam Kimber Rules AN0M App Was Not ‘Intercepting’ Messages, but Enabled Legal Police Surveillance.” *The Advertiser*, April 5, 2023.

Newman, Lily Hay. “Apple’s Decision to Kill Its CSAM Photo-Scanning Tool Sparks Fresh Controversy.” *Wired*, August 31, 2023.

Rankin, Jennifer. “Outrage over Girl’s ‘Drug War’ Death as Belgium’s Cocaine Haul Breaks Records.” *Guardian*, January 10, 2023.

PublicAffairs is a publishing house founded in 1997. It is a tribute to the standards, values, and flair of three persons who have served as mentors to countless reporters, writers, editors, and book people of all kinds, including me.

I.F. STONE, proprietor of *I. F. Stone's Weekly*, combined a commitment to the First Amendment with entrepreneurial zeal and reporting skill and became one of the great independent journalists in American history. At the age of eighty, Izzy published *The Trial of Socrates,* which was a national bestseller. He wrote the book after he taught himself ancient Greek.

BENJAMIN C. BRADLEE was for nearly thirty years the charismatic editorial leader of *The Washington Post.* It was Ben who gave the *Post* the range and courage to pursue such historic issues as Watergate. He supported his reporters with a tenacity that made them fearless and it is no accident that so many became authors of influential, best-selling books.

ROBERT L. BERNSTEIN, the chief executive of Random House for more than a quarter century, guided one of the nation's premier publishing houses. Bob was personally responsible for many books of political dissent and argument that challenged tyranny around the globe. He is also the founder and longtime chair of Human Rights Watch, one of the most respected human rights organizations in the world.

. . .

For fifty years, the banner of Public Affairs Press was carried by its owner Morris B. Schnapper, who published Gandhi, Nasser, Toynbee, Truman, and about 1,500 other authors. In 1983, Schnapper was described by *The Washington Post* as "a redoubtable gadfly." His legacy will endure in the

books to come.

Peter Osnos, *Founder*